WEBSITE FILTERING: AN EVALUATION OF LOCAL EDUCATION AGENCIES

A Thesis
by
ALAN MICHAEL WARREN

Submitted to the Graduate School
Appalachian State University
in partial fulfillment of the requirements for the degree of
Master of Instructional Technology

December 2010
Department of Leadership and Educational Studies

WEBSITE FILTERING: AN EVALUATION OF LOCAL EDUCATION AGENCIES

A Thesis
by
ALAN MICHAEL WARREN
December 2010

APPROVED BY:

_____
Paul Wallace
Chairperson, Thesis Committee

_____
Amy Cheney
Member, Thesis Committee

_____
Terry McClannon
Member, Thesis Committee

_____
Richard Riedl
Chairperson, Department of Leadership and Educational Studies

_____
Edelma D. Huntley
Dean, Research and Graduate Studies

Copyright by Alan Michael Warren 2010
All Rights Reserved

ABSTRACT

WEBSITE FILTERING: AN EVALUATION OF LOCAL EDUCATION AGENCIES

Alan Michael Warren, B.A., Western Carolina University

M. Ed., Appalachian State University

Chairperson: Dr. Paul Wallace

The idea of generating 21st century skills, which is an initiative for technology enhancement and global awareness, in a rapidly growing environment is challenging society with its sudden onset. As a result of this movement current and future students have a greater likelihood of possessing multiple jobs or careers that will require various skills and abilities. To provide students the best education possible, educators need to look at the barriers that are affecting technology use with the curriculum. Use of Web 2.0 tools, handheld devices, and other emerging technologies constantly in the midst of society forces technology directors to maintain a vision of persistent change.

One social issue currently affecting students is access to technology through the use of Internet resources. Some school districts implement tiered access to teachers (less limitations) and students (full limitations). Teachers who have access to tiered networks possess the ability to create a teacher driven learning environment without forfeiting mandated student protections. With tiered access, teachers utilize tools that would otherwise be considered inappropriate for use by minors to create valid educational resources.

Technology directors are provided many laws, doctrines, and resources at their disposal to help prevent access to inappropriate material from adults and students including the Children's Internet Protection Act (CIPA), E-Rate (provides federal

funding to local education agencies), Internet Safety Policies, Negligence, "In Loco Parentis," and "Local Decision." All of these laws, doctrines, and requirements are interpreted by the director of technology, or other authority in which he/she makes the final decision on availability to students. In most cases the technology director will make the day to day decisions regarding sources to be accessed at school. This study, consisting of surveys from twenty-one school systems and interviews of six technology directors, an auditor with the Universal Services Administrative Company, an E-Rate specialist, and a professor, will reflect on CIPA as it relates to the practices of the technology director.

Twenty-one technology directors in North Carolina were surveyed, with most of these directors holding degrees in areas other than technology. These are individuals who make the day to day decisions on which technological matter is considered to be educationally sound for students. Technology directors can cite any policy to determine a website invalid but based upon CIPA those policies could be over restrictive.

The research gathered for this study suggests that school systems and the state of North Carolina need to address current technology policies and trends to understand or possibly change how technology is implemented to students. The use of a committee to decide if web resources are appropriate, a tiered network that separates staff from student access to allow teachers to drive their instruction, and the implementation of state guidelines would create a uniform system for appropriateness of various technologies in schools. Most schools maintain close to one hundred percent Internet connectivity, and now is the time for school systems to utilize this technology to maximum potential.

List of Tables

List of Figures

Table of Contents

Introduction and Literature Review

Disclosure Statement

The researcher, at the time of publication of this thesis, is currently employed as an Instructional Technology Specialist for a school system in the state of North Carolina. Experiences shared with teachers and administrators regarding the restriction of Internet access in school settings generated the questions and concepts sought within this report.

Statement of the Problem

Due to economic conditions that have plagued the United States, during the first decade of the 21st Century, the people of the United States have demanded government agencies to become more transparent regarding policies and funding practices. The idea of transparency has forced government agencies to be more open to public record than previously before. In the field of education, the process of website filtration seems to become hard to understand and ambiguous. Technology has been pushed into the national spotlight as a major force, designed to improve educational learning in the classroom. A problem might be that students have little or no decision making opportunities regarding Internet access with which they best learn. Progress for Internet access in the realm of technology is inhibited by decisions being controlled by upper administration and local school boards. Some administrators attempt to point a finger at the government's legal system, claiming that various agencies under its umbrella are responsible for accessibility of specific technology in the classroom; however, there are laws that enable technology directors with the ability to invoke a "local decision."

> CIPA does not specify which filters must be used and stipulates that the filters can be disabled in certain situations for adult patrons. Under the

> law, local communities have latitude to decide what materials are inappropriate for minors, and the federal government cannot impose national standards in this regard. (McCarthy, 2004)

The "local decision" is a reference in CIPA that will enable the school board or superintendent the ability to appoint a position, usually represented by the technology director, to make day to day decisions.

School systems must follow regulations and standards created by the Children's Internet Protection Act (CIPA), E-Rate, and school boards of local education agencies (LEA) in order to protect students from accessing inappropriate information. These standards have led to heavy implementation of website filtering software that prevents students from accessing inappropriate material; however, when this type of filter is established, it also prevents teachers from accessing information that provide educational benefit. Through research, surveys, and interviews of varying agencies, this thesis will compare and contrast the rules and guidelines of the Children's Internet Protection Act and E-Rate with the roles and procedures created by local education agencies and their technology directors in North Carolina.

History and Background

CIPA is a broad law that regulates what content is available to be viewed by minors on the Internet. Within CIPA is a clause that gives a local school board, superintendent, or an appointed position (usually the technology director) the ability to maintain a "local decision" regarding what minors can view within the tenets of CIPA. "An authorized person may disable the blocking or filtering measure during any use by an adult to enable access for bona fide research or other lawful purposes" (FCC, 2009).

Due to the ambiguous wording of CIPA some districts provide a form or require an e-mail request, while other districts do not have a formal process in place allowing teachers to request access for bypassing a website filter. The question remains regarding who makes the decision to allow or deny a website to be viewed on a network established by a local education agency? If the decision is made to prevent a website from being viewed, are those who submitted the request notified with details why the website may not be viewed? Upon denial of a website's educational value, can the reasoning be viewed by the requesting party in a timely manner after submission? Questions such as these force school systems to remain transparent and provide reasoning as to their position to deny Internet access to teachers and students.

The basis of all these decisions should be focused on compliance with E-Rate and CIPA. The law and funding sources, such as E-Rate, that determine the compliance of a local education agency's network for CIPA should be the final factor when making a decision based upon Internet access in the classroom regardless of "local decision."

> (l) A determination regarding what matter is inappropriate for minors shall be made by the school board, local educational agency, library, or other authority responsible for making the determination. No agency or instrumentality of the United States Government may--
>
> (A) establish criteria for making such determination;
>
> (B) review the determination made by the certifying school, school board, local educational agency, library, or other authority; or
>
> (C) consider the criteria employed by the certifying school, school board, local educational agency, library, or other authority in the administration of subsection (h)(1)(B) of this section. (Wire or Radio Communication, 2010)

Per United States Code a school board, LEA, library, or other authority in the administration sector of a school system makes the decision on specific websites to be blocked or unblocked. While LEAs and administrators possess this right, are the

decisions to block Internet sites ever unfounded when they do not allow access to teachers or students?

Children's Internet Protection Act

CIPA was enacted in 2001 to protect children from dangers they could encounter when using the Internet. This law was created to enforce libraries and schools to limit Internet access to minors. In order to enforce this law, school systems and libraries could receive funding from the federal government through a program called E-Rate. The Universal Service Administrative Company controls E-Rate and will allot public funds to schools and libraries only if they comply with the rules of CIPA. The rules that CIPA require are:

> (B) Certification with respect to minors
>
> A certification under this subparagraph is a certification that the school, school board, local educational agency, or other authority with responsibility for administration of the school-
>
> (i) is enforcing a policy of Internet safety for minors that includes monitoring the online activities of minors and the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are--
>
> (I) obscene;
> (II) child pornography; or
> (III) harmful to minors; and
>
> (ii) is enforcing the operation of such technology protection measure during any use of such computers by minors. (Wire or Radio Communication, 2010)

This clearly states that a school system, regardless of personnel in charge, should protect minors from visual depictions that are obscene, child pornography, or harmful to minors. For technology directors interpretation of the law is imminent. The technology director has to decide upon appropriateness for student viewing. The legal definition for the terms visual depictions, obscene, child pornography, and harmful to minors are listed

in Title 18 of the United States Code. While there is no direct legal term for "obscene," the United States Code will reference Title 18 Sec. 2256 to guide the public on what can be considered obscene material. The North Carolina General Assembly makes a recommendation on how to define obscenity:

> (2) "Lewd matter" is synonymous with "obscene matter" and means any matter:
>
> a. Which the average person, applying contemporary community standards, would find, when considered as a whole, appeals to the prurient interest; and
> b. Which depicts patently offensive representations of:
>
> 1. Ultimate sexual acts, normal or perverted, actual or simulated;
> 2. Masturbation, excretory functions, or lewd exhibition of the genitals or genital area;
> 3. Masochism or sadism; or
> 4. Sexual acts with a child or animal. (Offenses Against Public Morals, 2010)

The term "harmful to minors" is discussed in Title 47 of the United States Code. This term is one that could be misconstrued and interpreted in many different ways.

> (G) Harmful to minors
>
> The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that--
> (i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
> (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
> (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors. (Wire or Radio Communication, 2010)

The focus of this portion of the "harmful to minors" section of CIPA has three requirements that must be met for a website to be deemed viewable. If a reasonable person would answer "yes" to one of these three stipulations the website would be

removed from use by minors. The first two refer to direct language regarding sexual material while the third points to the actual lack of educational value. If a website has any of the first two, the website should be blocked and inaccessible to minors; however, the last clause in this section refers to a lack of serious literary, artistic, political, or scientific value directed toward minors. A decision on the educational value is made usually by one individual. Due to the appropriation of duties within the hierarchy of local school administration, these types of decisions tend to be forced solely on the shoulders of the technology director. When these decisions are appointed to one individual, the decision may be based off of their own ideas and concerns.

In Loco Parentis

In Loco Parentis has been derived from English Common Law and has made its way into the American educational system. "It refers to an individual who assumes parental status and responsibilities for another individual, usually a young person, without formally adopting that person" (Phelps & Lehman, 2005). Technology directors have a right to invoke *In Loco Parentis* because when parents leave minors at school the school system becomes responsible for their safety. In terms of Internet safety, CIPA was created in order to protect children. CIPA gives appropriate direction and guidance to reasonable individuals regarding websites to be allowed in schools when students are using the Internet.

Although the school board has the overreaching authority to appoint who makes the local decision for Internet access within schools, that appointment will most likely go to the technology director. The technology director for that system might unknowingly create a hybrid point of authority by purchasing filtering software and thereby delegating

responsibility to a third party software company. The purchase of filtering software is a requirement of E-Rate in order to assure fidelity to CIPA. Filtration is a piece of software that is created and controlled by a company from another location. Technology directors place full faith in the filtering company and approve their decisions by invoking *In Loco Parentis*. By purchasing the software, school systems succumb to the thoughts and ideals of the company that support the software unless technology directors actively seek to monitor and unblock websites as appropriate. The "local decision" is rendered useless unless the technology director overrides the automated list given from the company.

Some technology directors may correlate the extent of website blocking to an appropriate amount of protection for their students when searching the Internet. If the school board appoints one individual to monitor student access to websites, that individual has become the *In Loco Parentis* in that school system. This thought contradicts the purpose of CIPA by implementing overprotection and allowing a limited process for teachers to properly teach their students in the classroom. The implementation of *In Loco Parentis* by a technology director is unnecessary when that school system has a technology plan and an Internet Safety Policy in place that must be followed in order to comply with E-Rate. If those policies and plans are properly in place, then teachers could invoke *In Loco Parentis* through classroom management techniques and govern their students appropriately. The teacher can align websites that contain educational value to the core curriculum thus allowing for increased teacher effectiveness.

In Loco Parentis has been challenged and defeated in court relating to arm bands supporting protest to the Vietnam War (Tinker v. Des Moines Independent Community

School District) and issues such as paddling students (Ingraham v. Wright). *In Loco Parentis* also had its share of victories, which include random drug testing in high schools (Veronia School District v. Acton) and the passage of the Gun-Free Schools Act of 1994. No legislation for *In Loco Parentis* thus far has related to website filtration techniques or the rights of administrators to invoke these tenets against websites which directly remove First Amendment rights from teachers.

What is a Website Filter?

A report in May of 2001, "Internet Filtering Options Analysis: An Interim Report" created for the InFoPeople Project, is similar to reports viewed by technology directors when CIPA of 2001 was enacted to comply with the rules of E-Rate. This report was generated to look at several website filtering software products and evaluate their efficiency and effectiveness.

> The ideal library filter would not block constitutionally protected speech and would only block "child pornography" or content that meets the legal definition of "obscenity." When it comes to library patrons that are minors, this ideal filter would also need to block "material that is harmful to minors ('harmful matters'). Recognizing that the distinction between content that is constitutionally protected and what is harmful to children is subjective and volatile is undoubtedly the reason filtering companies don't consider public libraries one of their prime markets. (Ayre, 2001)

Another report, "Internet Filtering Software Tests: Barracuda, Cyber Patrol, Filter Gate, & Websense" was created by the San Jose Public Library in April of 2008. This report

tested four software products to see if the accuracy of each product complied with the standards for which they were mandated.

In order to completely understand what a filter is one must first understand the inherent purpose of filters. The Internet filter is a piece of software that will allow school districts to limit access to students and adults. This software can be implemented in a number of ways giving school districts more ease in determining how websites should be filtered to their schools. "A network filter is installed on one central server and individual computers' settings are controlled by the settings on the server" (Houghton-Jan, 2008). These types of filters are the most common because the settings are implemented at the server and will filter down to each individual computer. The other types of filters that are available are those that are standalone filters which require software installation and individual settings on each machine. This would be a cumbersome process for even a small school district to attempt to implement and control.

Filters can block websites based on keywords within the URL, content on websites, file types, or pre-categorized lists set by the software company. Most school districts will use a product that comes pre-packaged because it is easier for the technology officer to open individual sites than to block all inappropriate pages manually. The report, "Internet Filtering Software Tests: Barracuda, Cyberpatrol, Filtergate, & Websense," suggests that while Internet filters protect against most obscene material there are still errors within the software.

> The accuracy rating of all of the various studies cited is 78.56%. The comparable sections of our informal student (keyword searching, direct URL access, RSS feeds, and catalog and database searches) yielded very

> similar results: an average accuracy of 76.29%, a difference of only 2.27%. (Houghton-Jan, 2008)

The findings of the report suggest that while Internet filters typically do their job, there are several websites blocked without a lawful reason to the purpose for blocking. While this report was generated for a library, all libraries and schools must adhere to the policies of CIPA and E-Rate if funding is received. Examples of websites found to be blocked by certain types of software were also listed in this report.

> **CyberPatrol–** WebMD, The American Urological Association, VictimsofPornography.org, Univision.com, DirtyPicturesBand.com (a rock band site with no adult content), Amazon and Google Book Search item pages (including the Amazon item page for an album by the band The Cure entitled “Pornography”).
>
> **FilterGate** – TheSmokingGun.com, Lesbian.org (a gay/lesbian support site), The Wikipedia entry for *Hustler* Magazine, a World War II History site, a UK breast cancer information site, entire blogs are blocked because of the many posts discussed something “adult.”
>
> **WebSense –** The report did not share specific websites regarding WebSense that were inaccurately blocked.
>
> **Barracuda —** Implantinfo.com (a site with a wealth of medical information about breast implants), PGLAF.org, a Gay.com article on queer sexuality and another on “Our Trans Children”, a Nazi History Article, Hustler’s Home Page, Lesbian.org (a gay/lesbian support site), SexHelp.com. (Houghton-Jan, 2008)

This report is only a fraction of the material that can be found in the library or Internet related to website filtration software. Most software will be prepackaged by the company that created the product. When software is prepackaged the blocked lists are often set by category depending on keywords, domains, and graphic content that may appear on a webpage. This allows for school systems to purchase the product and will allow the software to block websites a third party deemed necessary. Under this premise the technology director has permitted a third party to decide what is not appropriate to minors. CIPA states that determination of appropriateness must be a local decision appointed by the superintendent or the school board of education. The third party (website filtering company) has now become the stakeholder and can influence the student's Internet education capability.

Third Party Website Filter Software

When third party sites are allowed to create block lists that come prepackaged, the technology directors can gain a false sense of security. When technology directors feel that everyone is protected, they inadvertently give the software company the edge when it comes to local decisions.

> Having released themselves from the need to service public libraries whose legal predicament is much too murky, the filtering companies are free to devise filters based on language that works for their target audience – parents, employers and schools. Therefore, you'll never see a category of websites defined as "harmful matters" or "child pornography". Some take the plunge and define websites as "obscene" but how closely those websites match the legal definition is anyone's guess. And since none of the

> companies release the list of websites on their radar and the category into which they've been placed, the end user has no way of knowing whether the "obscene" sites include some Constitutionally protected sites or not. (Ayre, 2001)

Software companies hold information as proprietary to the business so owned lists cannot be hijacked by similar companies. Technology directors always have the right to go into the software package and unblock sites previously blocked on the prepackaged list, but most directors wait for teachers to find websites needing to be unblocked. This is important because technology directors are not proactively opening up resources for teachers.

When a technology director is not proactive and constantly seeking websites to unblock, the software companies maintain a foothold on public access of Internet use in schools. Websites that do not align to the three requirements of CIPA become subject to the rules of the company. When this scenario appears, a company could make "local decisions" without the approval of a board, committee, or the technology director; this company could be based in another area of the country or another part of the world. Technology directors still maintain responsibility for manipulating the software but when the technology director does not override the list, the software company has control.

Internet Safety Policies

"Applicants must enforce a policy of Internet safety and certify compliance with the purpose of the Children's Internet Protection Act (CIPA) to be eligible for discounts" (Universal Services Administrative Company, 2010). All school systems who receive E-Rate funding must have an Internet Safety Policy that was approved by the board and was

open to public comment upon its inception into school system operations. Most school systems will maintain a generic Internet Safety Policy stating what a teacher, student, or other network user must adhere to in order to comply with the rules and regulations of E-Rate. An Internet Safety Policy will rarely require a school system to post options for requesting to view a site that is currently blocked by website filtering software. An Internet Safety Policy should have the restrictions of the network listed but it should also include methods for teachers to appropriately request websites to be marked for review.

Most school systems have a process in place to identify and review websites. However, most of those school systems fail to provide a form that will allow teachers to request websites to be opened. There is no provision for a review committee or a method of feedback that can adequately supply teachers with the information needed to be successful in the classroom. In some districts, the technology director is the sole decision maker determining when to unblock a website. In other districts, it may be a committee, instructional technology employees, or curriculum directors within the system who make the decision as a team. Acceptable use policies created by districts are similar because collaboration allowed for the creation of those documents. As a result of CIPA, technology directors possess the authority to make a local decision without having any formal body to review those decisions including, but not limited to, the superintendent, school board, or parents.

The Internet Safety Policy must address the following issues:

- Access by minors to inappropriate matter on the Internet and World Wide Web.
- The safety and security of minors when using electronic mail, chat rooms, and other forms, of direct electronic communications.
- Unauthorized access including “hacking” and other unlawful activities by minors online.

- Unauthorized disclosure, use, and dissemination of personal information regarding minors.
- Measures designed to restrict minors' access to materials harmful to minors. (Universal Services Administrative Company, 2010)

Through E-Rate, the wording of CIPA has been reduced from containing phrases "obscene," "harmful to minors," or "lacking serious educational value" to "inappropriate matter" in an attempt to simplify understanding for school systems. Inappropriate matter has a number of definitions that could be associated, and when the "local decision" must be made by one individual to assess this matter, the interpretation becomes murky.

E-Rate

"E-Rate – more precisely, education rate – was enacted as part of the Telecommunications Act of 1996 and a new aspect of universal service programs in the U.S." (Bertot, 2000). E-Rate is the process created by the Universal Services Administrative Company which is regulated by the Schools and Libraries Division (SLD) to provide support to low income school systems and libraries to help fund Internet and telecommunications equipment to the public.

"The goal of E-Rate is to provide connectivity to network services through universal service principles as presented in Sec. 254 (b) of the Telecommunications Act of 1996" (Park, Hansa, and Jing, 2007). The process that an LEA must follow to receive discounts from E-Rate is to "prepare a technology plan, opening the competitive process, seeking discounts on eligible services, confirming the receipt of services, and invoicing services" (Park, Hansa, and Jing, 2007). Once complete, in order to retain funds for Internet access, auditors contracted from E-Rate investigate the filter. This is done to confirm that the filter is indeed working properly (preventing pornography), so the government can guarantee that the software purchased is in fact used appropriately and

complying with federal law. Anything purchased that will enable Internet access with E-Rate funds must comply with the requirements of a filter attached to the network.

Overall Purpose

The purpose of the research is to determine if CIPA limits rights to teachers or if policies and processes set by local education agencies work outside of the interpretation of CIPA thus limiting rights to teachers. Technology directors from various school systems must purchase website filtration software and safeguard our students from inappropriate material. With little to no research published yet in this field, questions arise as to how technology directors make their decisions regarding website filtration software. Therefore, the following research questions were formulated for this present study: (1) What are the appropriate guidelines that technology directors should follow when establishing criteria related to appropriate website? (2) Do technology directors or appointed committees with authority to approve websites base a local decision on the tenets of CIPA? (3) How does the "local decision" of technology directors differ from system to system regarding website access to teachers?

Methodology

Characteristics of Subject Population

In this section the characteristics of the participants in the study will be discussed. Technology directors and their current policies towards webpage access to teachers are the primary focus of the research. Directors were surveyed and a few will be selected for a personal interview to gather data of specific school systems. An E-Rate specialist and an E-Rate auditor discussed the processes in place to determine the legitimacy of policies and appropriate allocation of funding to school systems. A university professor, who educates in cyber law, discussed CIPA, E-Rate, and school board policies.

Participants. The participants for the study were selected by the use of two methods. The first method was a survey created in Survey Gizmo that would blanket the state of North Carolina requesting information from school systems regarding website filtration processes. This method was used to gain baseline data that showed how school systems make decisions about website access in schools.

The second method was a set of interviews that included six school system Technology directors, one E-Rate Specialist, one E-Rate Auditor, and one professor that specializes in Cyber Law in the University System of North Carolina. The technology directors have been chosen by proximity to the researcher and have been selected solely on the willingness to perform an interview for this study.

Other interviews include an E-Rate Specialist, E-Rate Auditor, and a professor who have been contacted via e-mail or phone. Willingness to accept an interview after the initial disclosure of the study confirmed selection. No individual contacted was of a

prior acquaintance to the researcher and all participants were either recommended or contacted by the researcher to obtain permission to interview those individuals.

Survey participants. The survey delivered to the technology directors was a broad reaching data gathering tool sent to one hundred and fifteen school systems in the state of North Carolina. The questions were meant for the technology director or the position that makes the day to day decisions regarding website filtration software in public schools. The responses received were analyzed to understand the variance of degrees of these individuals and their ideology on issues affecting website filtering in schools. All responses were considered to represent the school system in which those directors are affiliated.

Chief technology officer. Six school systems were chosen based on proximity to the researcher's location. The questions to the interviewees were in-depth and were not intended to be the responses of an individual but the responses of the school system. All persons interviewed were assigned a random number to allow identification of school systems while protecting identification of the individual interviewed. The responses from these institutions allowed for an in-depth view of how technology directors decide on relevant and irrelevant educational decisions.

Technology directors were contacted via e-mail to gain interest in the participation of this study. If anyone in the pool of directors responded positively, then those directors were contacted again for the purpose of scheduling an interview. The technology directors were asked twenty questions that relate to the school system's position of specific websites, Internet safety, and E-Rate compliance. Each interview was conducted in the interviewee's offices and concluded in a time period of fifteen

minutes or less. Information regarding attendance and demographic statistics from the NC School Report Card systems can be found in Appendix H through Appendix M.

E-Rate specialist. The E-Rate Specialist that was chosen was contacted via e-mail and asked a series of questions related to utilization of E-Rate and specific E-Rate requirements that schools must complete to remain compliant and receive funding from the government. The E-Rate Specialist selected is with the North Carolina Department of Public Instruction based in Raleigh. The specialist was asked several questions related to website filters in North Carolina schools and auditing processes by the government for the compliance of E-Rate funding. The interviewee was allowed to answer questions and return the responses via a word processing document.

E-Rate auditor. The E-Rate auditor was selected from the Schools and Library Division which is a federally run organization set up through the Universal Service Administrative Company. The auditor was asked a series of questions in which a response was given via a word processing document. The auditor was asked several questions regarding selection of a school system for audit and types of websites searched when checking the website filter for its overall effectiveness to protect students per CIPA.

Professor. The professor is an active educator in the University of North Carolina system and is qualified to answer all questions regarding cyber law as it relates to minors and the public school setting. The interviewee was asked questions related to the CIPA. The questions were specifically related to the sections of CIPA related to "harmful to minors," "obscenity," and "the local decision."

Procedure

Survey. A survey was conducted to one hundred and fifteen school system technology directors. The survey was created in Survey Gizmo and consisted of twenty questions related to website filtration and processes implemented by technology directors. Survey Gizmo is a web based application that allows researchers to implement a survey to participants via a web link. Survey Gizmo gives the researcher the option upon release to refrain from tracking participants through Internet protocol or Internet cookies. This prevents an outside source from tracking down identities based on results if data were to be compromised. This survey will aid the research because it allows the researcher to gain a baseline of information that will fuel questions given to interviewees. Participants accessed the survey through a website link through the list serve for North Carolina Technology directors set up by the North Carolina Department of Public Instruction. These technology directors by opening and completing this survey were willingly participating in the survey and results were to be compiled and analyzed. The researcher has submitted and received information from the Institutional Review Board (IRB) stating that it does not constitute human subjects research and does not require IRB approval (Appendix B).

Technology directors. Six technology directors were contacted by the researcher to gain an interest in the participation for an interview. Technology directors were chosen based on proximity to the researcher's current location. When technology directors responded with interest then a time and date was established for an interview to take place at the office of the interviewee. Questions asked in the interview related to Internet

Safety policies, Children's Internet Protection Act, E-Rate, and processes for teachers to request a website to be unblocked for district use.

Professor. The professor is an educator who specializes in public school law and currently educates in North Carolina and is knowledgeable of elementary and secondary legal issues. The interviewer asked several questions that related to laws and their interpretation that directly affects public school education.

Auditor. An auditor who has conducted sixty-six audits on school systems based on the E-Rate auditing process was contacted for an interview. The auditor selected for the interview works directly with the Schools and Libraries Division with the Universal Service Administrative Company based out of Washington, DC.

E-Rate specialist. A North Carolina E-Rate Specialist with the North Carolina Department of Public Instruction was contacted. The E-Rate specialist has a working knowledge of what school systems may allow based on the guidelines set forth by E-Rate.

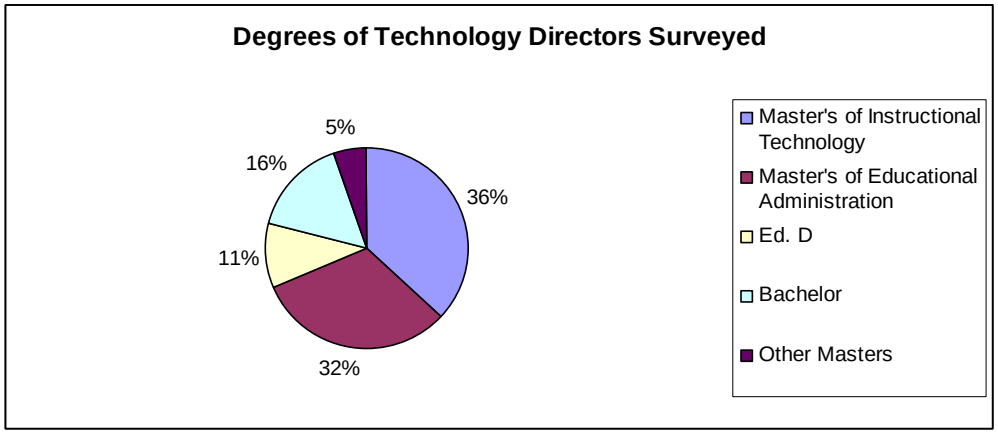
Results

Survey

Technology directors. One hundred and fifteen technology directors were contacted through an e-mail list serve that is operated by the North Carolina Department of Public Instruction to participate in a survey. Twenty-one responses were received and analyzed from the directors who chose to participate in the survey.

Figure 1.1 shows that of twenty one responses, 36% held a Master's Degree in the field of Instructional Technology. There were no responses given that would signify that any of these individuals held a doctoral degree in the technology field, nor is it a requirement to have a doctoral degree for this position. Some directors responded that they hold a degree in administration, management information systems, or had a regular curricular degree such as Biology, but gained a certification to work with technology.

Figure 1.1

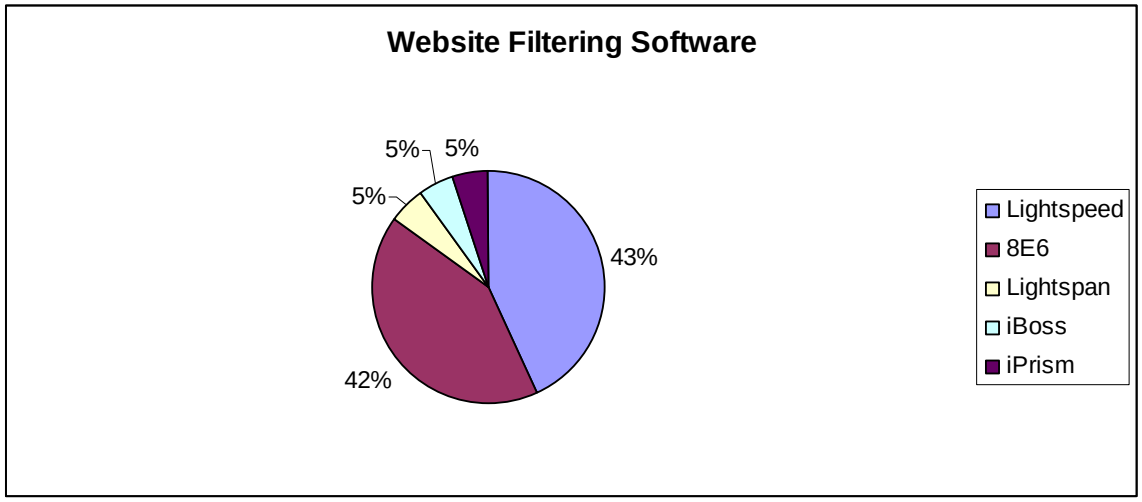


Technology decision makers. While many directors have control to make immediate daily decisions regarding what websites can be approved or denied, there are some that have selected the use of a committee to make these decisions. The survey

found that 86% of technology directors make daily decisions regarding Internet websites in use in schools.

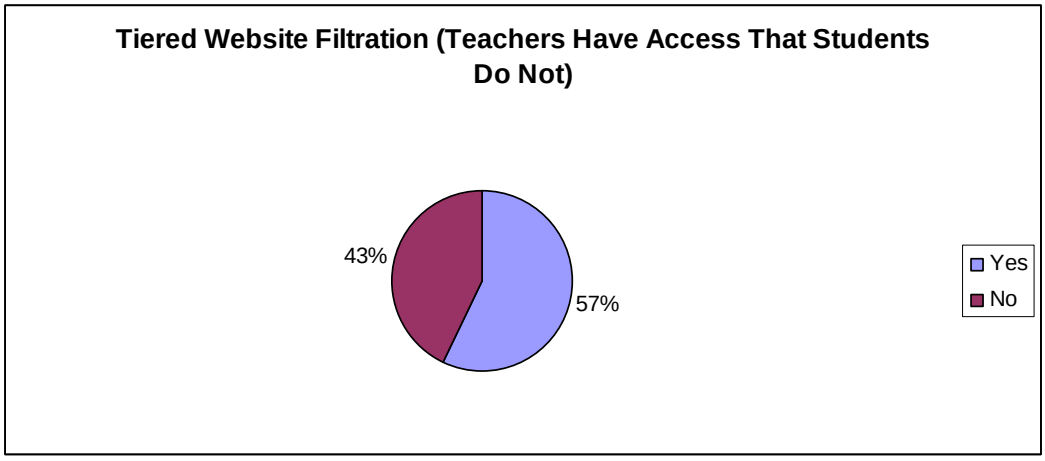
Website filtering software. Figure 1.2 demonstrates that respondents to the survey use varying types of website filtering software which include 8E6 also known as Marshall 8E6, Lightspeed, Lightspan, iBoss, and iPrism. All respondents to the survey reported that they had some sort of a website filter in use on their network. The majority (43%) reported using Lightspeed, with Marshall 8E6 (42%) being nearly as popular. These two programs represent 85% of the website filtering software reported in this survey.

Figure 1.2



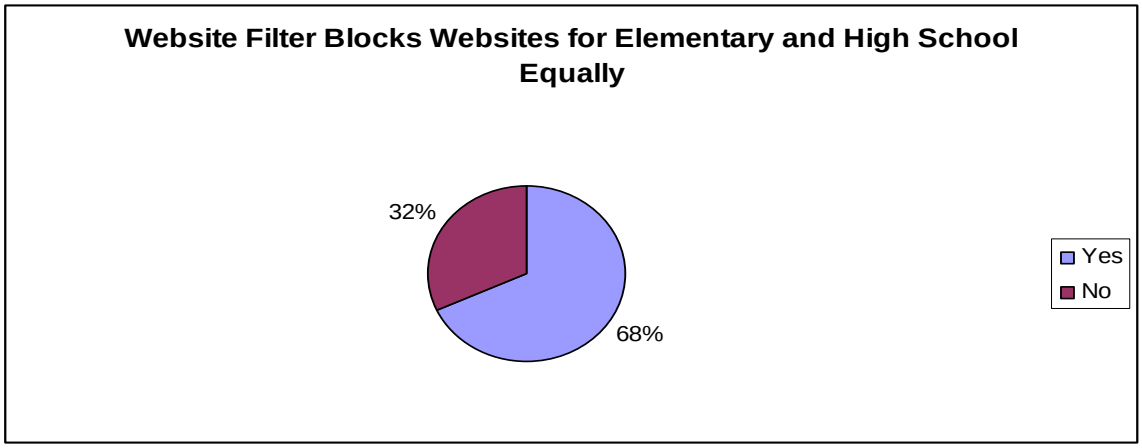
Tiered website filtration. Figure 1.3 demonstrates that of all the respondents, 57% allow teachers a different form of access to the Internet than students. For most school systems, for example, this might allow the use of social networking websites to teachers, but completely denied access to them by students.

Figure 1.3



Elementary to high school filtration. Figure 1.4 demonstrates that while some schools provide separate access for the teachers, 68% do not segregate their networks allowing for age appropriate access at elementary, middle, or high school environments. This would imply that elementary students at these locations have the same access to websites that high school students have.

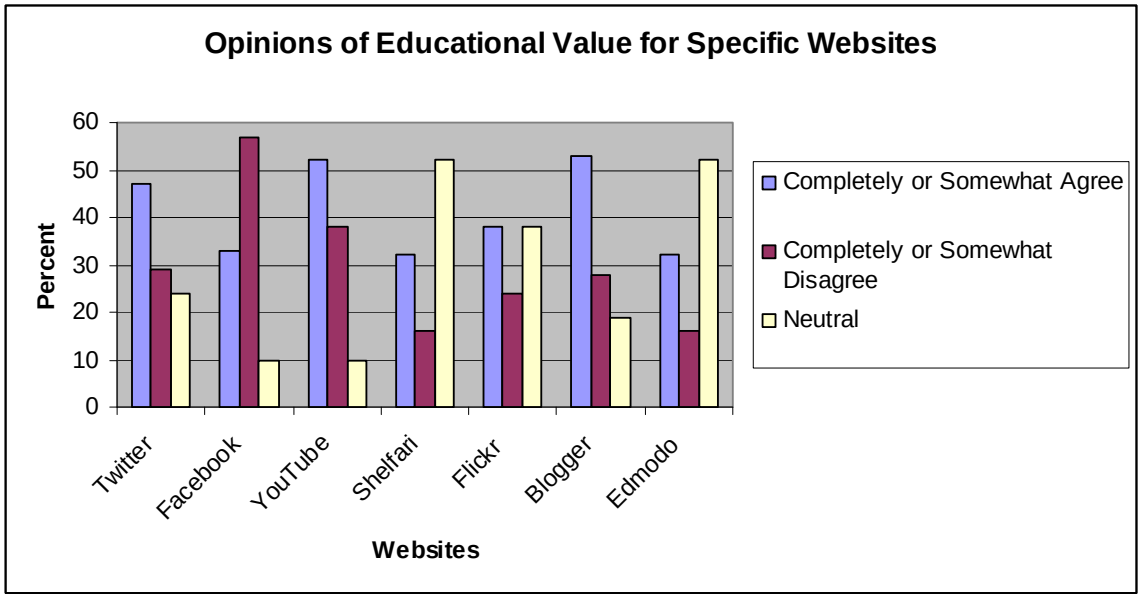
Figure 1.4



Statistical breakdown of specific websites. Table 1 lists the results of questions asked about the opinion of technology directors regarding specific websites. These responses are not to suggest that these technology directors currently have approved or

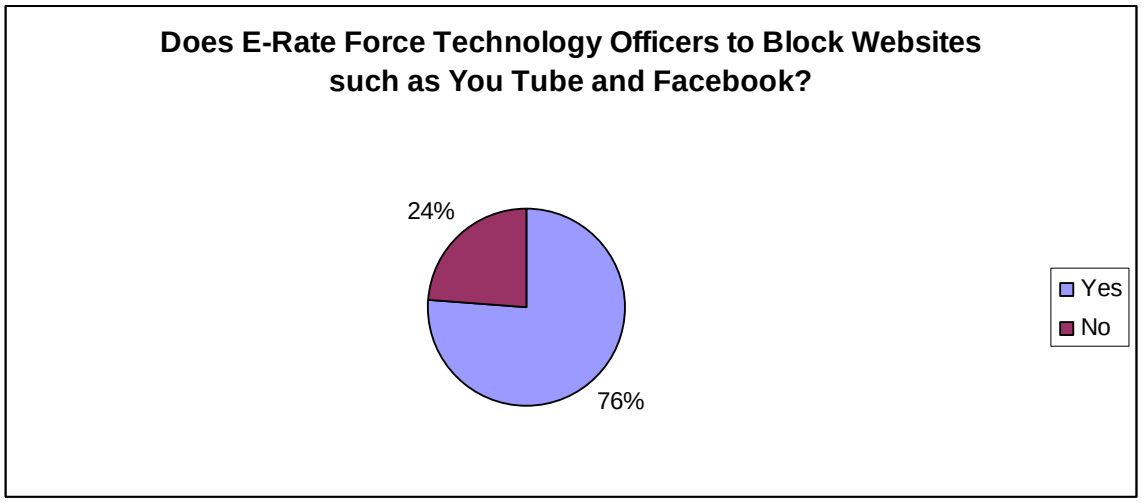
denied these websites. Some technology directors have these websites open but do not agree with the current use of the website in the educational setting. Respondents were asked to choose “completely agree,” “somewhat agree,” “neutral,” “somewhat disagree,” or “completely disagree” when answering the questions.

Figure 1.5



Technology directors vs. E-Rate. Figure 1.6 shows the question asked to technology directors regarding E-Rate, and whether or not it prevents them from allowing students to access websites such as YouTube and Facebook. Out of the twenty-one responses given, 76% of all the technology directors believe that E-Rate has a direct effect on the approval of websites that could be considered social networking.

Figure 1.6



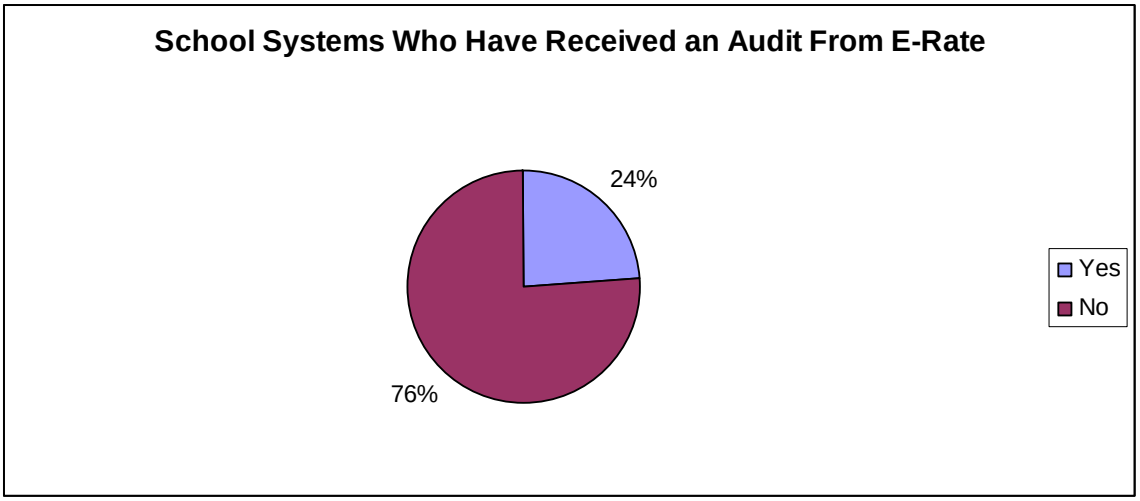
Approved Websites in School Systems. Websites chosen for the survey were to represent a varying degree of social networking websites based on those websites marketed to education and those that are public based. Websites such as Edmodo are set up so that teachers and students can have a safe area to communicate and guide instruction. Facebook is for checking up with your friends and viewing status updates, and, therefore, may not be considered an "educational outlet" by directors. Table 1 is a graphical example of those responses.

Table 1
Approved or Denied Websites

Website	Yes	No
Blogger	33%	67%
Wikispaces	86%	14%
Facebook	19%	81%
Twitter	48%	52%
YouTube	43%	57%
Flickr	38%	62%
Shelfari	52%	48%
Edmodo	48%	52%

Audits from E-Rate. Figure 1.7 demonstrates that of the twenty-one respondents only 24% of the school systems actually had an audit from E-Rate. The survey does not address if a school system ever lost E-Rate funding, but the overall practice of auditing since the inception of E-Rate shows that E-Rate can choose a school system at random. The frequency of an actual audit has been low over the past nine years.

Figure 1.7



Internet safety policies. All school systems surveyed comply with E-Rate by having an Internet Safety Policy that explains the guidelines of network use. No school system who participated in this survey failed to comply with the orders of E-Rate based on the implementation of an Internet Safety Policy and a website filter. Ninety-five percent of the school systems surveyed held teachers and students accountable when there was a direct violation to the Internet Safety Policy. It is hard to discern if the remaining five percent really does not hold faculty and teachers accountable when they break school board policies.

Interviews

District #1 (Appendix B). Teachers or students have an opportunity to send a request to the Technology director. If a teacher tries to access a page that is blocked,

there is a form in the blocked page that will allow the teacher to request access. That website is then reviewed by the director and a decision is made. The director will seek guidance from principals or other members of administration. However, the technology director will usually make the final decision regarding what can and cannot be blocked.

The return time for requests will usually take a day for review. This school system is a one-to-one initiative system that allows students to take home a laptop for grades four through twelve. The Internet Safety Policy for most systems list everything that a user cannot do on the Internet but fails to let teachers know that they can request access to Internet sites if they are determined to be in compliance with CIPA. This director does not usually reference CIPA when teachers are denied access to a webpage because they feel their Internet Safety Policy references the rights of the teachers.

The technology director for this district does not block websites based on general advertisements as long as the advertisement is not pornography. The filter is set up to look at content on a page and decide what is appropriate and what is not as it relates to minors.

When asked about the “harmful to minors” and “obscenity” clauses as it relates to the protection of minors in the district, the director referred the researcher to the Internet Safety Policy of that district.

The director was then asked a question about the validity of Facebook and its potential violation of CIPA.

> I do not know that we would call it a violation of CIPA but we block it because of the issues that it causes. It causes problems with kids writing stuff about other kids. We do not really have gang problems but just

> cyberbullying. We block all the social networking sites. We actually had Twitter unblocked for a while because a high school principal wanted to use it but the kids started using it to cheat so we had to block it. (personal communication, July 20th, 2010)

Facebook is blocked in this district and the director states that Facebook and Myspace have "zero educational value." To counter this opinion, the director was asked if other social networking sites were open such as Edmodo and Ning. The director responded with both websites being unblocked, with Ning being used and no one actively using Edmodo.

This school system considers YouTube to be a violation of CIPA because "there is too much obscenity out there" (personal communication, July 20th, 2010). When the interviewee was asked if this webpage lacks serious literary, artistic, political, or scientific value as to minors they responded, "There is good stuff on YouTube but there is a lot of inappropriate stuff too. Our filter is all or nothing." This school system uses M86 filtering software and it does not allow the director to differentiate between what is available to students and teachers.

This school system has not received an audit from E-Rate but does have an Internet Safety Policy. This system does have a course available to students, teachers, administrators, and parents regarding digital citizenship and its core components.

District #2 (Appendix C). Teachers or students who access a website that is blocked will receive a message from the website filter that will tell them the website has been logged. On the page that reports the website being logged or recorded, a teacher or student could then click the link to fill out a form. This form requires contact information

and information as to why a teacher or student needs access to this site. Upon the submission of this form, the technology director will receive an e-mail and can access the webpage in question to make a call almost immediately.

Teachers are told that blocked content violates the Internet Safety Policy if they submit a Website Request form for a website that the technology director would deem inappropriate. If an administrator submits a request that is denied, then that administrator will receive a response based on CIPA. The director feels that teachers do not need to worry about the constraints of CIPA unless the teacher wants to know why directly.

Advertisements are blocked based on category and the director feels that the website would not display correctly with advertisements such as Viagra. Websites must be filtered in such a way that the "harmful to minors" section of CIPA is complied with at all times.

> Harmful to minors has no set policy here but it is in my best interest to protect kids. Of course porn is blocked. YouTube and MySpace have inappropriate and foul language along with anything that you think is unethical. We would try to block it. So that is basically my call. We have keyword blocking on our filter that works well and it enables the Google Safe Search and other search engines with the software that they provide. (personal communication, July 27th, 2010)

Facebook, in this school system, is considered to follow a fine line because the director allows teachers and administrators access to Facebook while the system denies students access. "Teachers are on a different network because they are on laptops. All teachers have laptops. The wireless network is free reign except for porn. The kids are

hardwired and they are on a different network. So that is how we segregate it out." (personal communication, July 27th, 2010)

The director notes that LEAs have the final decision when it comes to what websites are open or not regarding social networks.

> I think Facebook is good when it is used for good but you know there is always a negative with the positive. I think it is overkill as far as information. Of course for teachers, adults, and kids that is how they communicate these days. For us as a school system to keep up with so many communication portals because we have a website, email, Facebook, YouTube, Twitter. There is just so much to keep up with. I suggest to all directors that yes it is good to do Facebook but we are double doing our work. Just point everyone to our webpage and there you go. (personal communication, July 27th, 2010)

Due to the validity being in question for other social networks, this school system has invested its time into its own web 2.0 website (SchoolFusion) to help teacher and students do what they wish in a safe environment.

YouTube is open for teachers and administrators but not for students because students have an option of using SchoolFusion to fulfill those needs.

> SchoolFusion has web 2.0 tools so we do have video that we can upload there as well. I always try to make it simpler. I mean sometimes you have to take a few more steps to go to SchoolFusion but it is better than students going to YouTube and getting in trouble. (personal communication, July 27th, 2010)

This school system has never been audited by E-Rate and maintains an Internet Safety Policy explaining the guidelines of the network. This school system has information ready for students regarding cyber bullying based on the new law. They do not have any other material ready to share with teachers or students regarding the rest of the core components to Digital Citizenship such as Internet safety or copyright.

District #3 (Appendix D). Teachers can submit a request to a filtering committee. This committee will take the website and review to see if it violates guidelines as established by the school system.

> A filtering committee will take a look at it and if it is an obvious violation of rules and regulations then they deny it. If it is obvious that it is appropriate then they will open that site. If it is in the gray area in between then it gets bumped over to me, and I will take a look at it and try to determine whether it is appropriate for teacher or students. We do have a dual filter in which adults are filtered differently than students. (personal communication, July 29th, 2010)

Teachers are given feedback when a website has been denied permission for access. The Internet Safety Policy is referenced when discussing the inappropriate behavior of the website.

This school system does allow different filtering to take place between students and teachers, which allows for more websites to be accessed by adults.

> While we may open, we still are not going to open a site just because someone requests it. It is going to have to be something that is educational. Typically some of those sites they have asked to be unblocked because of

> the funny ways that filters will sometimes work a lot of stuff from universities and the like will end up on the blocked list just because the filter defines it that way. We try to be sensitive to folks for research and those sorts of things and do open those sites for those adults, but just because you ask does not necessarily mean it will be opened. There are always home computers and libraries for things that are questionable. (personal communication, July 29th, 2010)

This school system does not block websites based solely on the use of advertisements on a webpage.

> It is one of the big concerns I have with YouTube. YouTube is open for adults but not for students. One of the concerns I have with YouTube is teachers who are going to log in under their name are going to have it on a projection system. I was at a location where a school was doing that and there were no children in the room but up pops an ad for Cialis. The other thing that bothers me is the comments that are there. I have seen comments that are pretty inappropriate for kids. (personal communication, July 29th, 2010)

The school system approaches "obscenity" and "harmful to minors" by using a dynamic filter. As soon as a student, teacher, principal, or any other user logs on to a computer, the Internet Safety Policy will pop up and will require the user to accept. If the user refuses to accept the Internet Safety Policy, then the account is disabled. "We get more requests from teachers to block sites than to unblock sites" (personal communication, July 29th, 2010).

> This system does not have Facebook available to teachers or to students. We had a teacher who was fired for comments they were making about students on Facebook. We understand that there are some educational values to social networking and I think we are going to have to do some type of social networking. I think that is what everyone is struggling with now is trying to find what is appropriate and how to protect students in that type of environment. Some things we are looking at are the implementation of a moodle and we have a wiki that we are using to allow teachers and students to talk appropriately about assignments or readings. We are trying to put some tools out there rather than going the full blown route. It is a real slippery slope. (personal communication, July 29th, 2010)

This school district only allows LinkedIn to be accessed by teachers and there is no negotiation as to the allowance of social networking in the schools.

The school system has received an audit from E-Rate but that organization has never pulled funding for non-pornographic sites being available to students. The Internet Safety Policy is in compliance with the rules of CIPA and E-Rate. There is a cyberbullying program, which promotes awareness to teachers and students, in place for this district. The media services department does a discussion with teachers and students based on all forms of copyright. "I would like to see a stronger focus on the Digital Citizenship strand because obviously Career and Technical Education does not hit every child. I think we have as much problem with adults, in some cases more, than we have with students in understanding what copyright is" (personal communication, July 29th, 2010).

District #4 (Appendix E). When teachers in this system encounter a blocked webpage, teachers will e-mail the director a link to the site with the reason why they want a webpage to be open or not. When a webpage is blocked, the director will receive a report through the filter software and can either approve or deny the website. The process is informal but the director claims that the turn around time is about twenty-four hours. If a website is deemed inappropriate, then the director will e-mail that teacher explaining why a website will remain blocked.

> I just explain it, like in the case of iTunes the main reason is we do not want students downloading to their iPods and then we have to deal with all the things they downloaded. Sometimes bandwidth is an issue and a lot of time teachers are not asking for websites to be opened that are not educationally appropriate. A lot of my denials have to deal with the wireless network and bandwidth. (personal communication, July 28th, 2010)

When providing feedback, the director will reference CIPA if it is appropriate for the website being reviewed.

This school system does not block websites based on advertisements, but the filter itself will block content on the webpage that is deemed inappropriate.

> This filter also provides us with an educational video library. Teachers can submit videos at YouTube that they want students to be able to access and then I put the link in the educational library. When students access the video from the library it plays without all the surrounding stuff around like all the suggestive videos because that is hard to block. Everyone loves YouTube

> and we don't want to take it from them. (personal communication, July 28th, 2010)

This system allows teachers and students to have access to YouTube except on the wireless network.

> I like to give teachers the freedom they need to teach what they need to teach. All the resources they can grab because who am I to tell them what works. Displaying something and having students face to face with something are two different things. I want to be in a teacher driven system. I am in a Chief Technology Officer program with the state and we go to these classes and some superintendents don't want to block anything for anybody except porn because they don't want to tell teachers what to do. It's funny because you have the other side where we are going to block everything and you tell us what you need. But, how are they supposed to find what they need without access? (personal communication, July 28th, 2010)

This school system does block Facebook. "Social networking has a place but we are not convinced that Facebook has a place in school. We have a couple teachers who have been exploring using Ning and they were really good with it but we transitioned to a new website platform called E-Chalk that gives teachers more tools" (personal communication, July 28th, 2010). This school system is open to social networking and continues to allow teachers and students the ability to access the educational version of Ning.

This school system has received an audit from E-Rate but has not had any funding pulled from the system related to websites that are non-pornographic in nature. The system is currently exploring programs to communicate Digital Citizenship to faculty and students.

District #5 (Appendix F). Teachers will make a request to their Instructional Technology Coordinators who will then review the website and make a decision as to its educational value. If approved the director or facilitator will take the website and fill out a form that is sent to the firewall engineer. This engineer will open the site on the website filtering program to allow teachers access. "The engineer always e-mails back and says it is open or we can not open it because…and gives the reason why" (personal communication, July 26th, 2010). The Internet Safety Policy included CIPA language to allow adults to circumvent the filter in order to do research. This school system does not prevent access to websites based on advertisements that may be on a webpage.

This district takes an open approach when determining the definition of harmful to minors.

> The interesting thing about "harmful to minors" is who determines what harmful to minors is. The way that we have understood the language is that it is based upon the mores of your particular area in which you live. We tend to try to leave everything as open as we can unless we get a specific complaint about it." (personal communication, July 26th, 2010)

When discussing obscenity the director shared the stance of the school system and what they consider to distinguish appropriate websites for minors.

> It's referring specifically to graphics/pornography and obscenity is looking at graphics more than language. There again we try to operate based on the accepted practice within our community here and if we get complaints we look into it. We do have teachers contact us from time to time saying "this is offensive." We look at it as a community to decide if it is truly offensive because what is offensive to somebody may not be offensive to somebody else. Without a clear definition, the Supreme Court is saying they can not define it but they know what it is when they see it. It really leaves it open to interpretation. (personal communication, July 26th, 2010)

The point of view when addressing the educational value of Facebook was based solely on the age of the students.

> Facebook, under its terms of agreement, you are not supposed to be under thirteen. There is no way for us to differentiate that to our students. In light of that, we give access to our teachers for Facebook. Our staff Internet Safety Policy says that they can make school related Facebook accounts on which they can post announcements to parents but it is not to be for the dissemination of any other curricular information. That should be posted on the district webpage. (personal communication, July 26th, 2010)

When asked about the literary, artistic, political, or scientific values as to minors as it relates to Facebook the director responded, "Aside from the terms of agreement for Facebook it is classroom management that drives that. Teachers complain bitterly that the students are on Facebook at inappropriate times. That is a classroom management issue not a CIPA issue" (personal communication, July 26th, 2010). Social networks are

looked at on a case by case basis for their educational validity. “You have to do that because they evolve and change so quickly. Our Internet Safety Policy does not reference Facebook particularly; it states “social networking” in a general format to cover that website” (personal communication, July 26th, 2010).

YouTube is currently blocked by this school system to students but teachers and staffs have access to these websites. “There is value out there. There are wonderful teaching materials that are out there but because there are also so many inappropriate materials that are also out there we have limited access to staff” (personal communication, July 26th, 2010).

This school system has received an audit from E-Rate but has never had any funding removed due to being in non-compliance of their filtering software requirements. This school system has an Internet Safety Policy in place and does not currently have a formal course in place to explain to teachers or students regarding Internet safety, ethics, or copyright.

District #6 (Appendix G). Teachers make a request to the director of technology online. These websites are then reviewed and either allowed or denied by the technology director. Teachers are sometimes given reasons as to why a website is not approved but is handled on a case by case basis. “Perhaps it is a website that contains malware to which they are not aware of in which we inform them of that and if it is a site that has objectionable material we have to look at the circumstances” (personal communication, July 27th, 2010). If a website is deemed educationally related, the system will allow the website. This school system does not block websites solely based on advertisements on a webpage.

When asked about “harmful to minors” and “obscenity” and how the school system protects these students the director replied, “I guess common sense societal standards, I suppose. The filter has its own categorized list content types and for the most part follow that. There would be a difference between sex based websites and sex education websites” (personal communication, July 27th, 2010). The director then said, “Our ability to filter is only as good as the technology available” (personal communication, July 27th, 2010).

Facebook is not considered a violation to the tenets of CIPA but is blocked by the district completely because the district does not use the site as an educational tool. When asked how the website relates to serious literary, artistic, political or scientific value as to minors the director responded, “It’s just blocked because we have not had any educational value in using the site” (personal communication, July 27th, 2010).

When asked about the educational value of Edomodo and Ning, the researcher received a similar response. “Again based on the perceived educational value it is looked at by administrators and decisions are made accordingly. Your filter abilities are only as good as the technology available” (personal communication, July 27th, 2010).

This school system has been subject to a selective review through E-Rate but has never lost funding due to social networks being available to teachers or students. This school system does have an Internet Safety Policy and does not have a formalized course in cyber bullying or Internet safety. The director stated that there were several other methods available where students could receive this training.

Summary of Interviews

Table 2
Interview Summary

	District #1	District #2	District #3	District #4	District #5	District #6
Dual Filter.		X	X	X	X	
Blocking social networking to students and teachers.	X	X	X		X	X
Block some social networking to teachers.	X		X	X		
Do not block any social networking to teachers.		X			X	
Received an E-Rate audit.			X	X	X	X
Cyberbullying program established	X	X	X			
Has a committee to determine educational value of websites			X		X	

All of the directors interviewed developed interesting conversations that permitted the interviewer to acquire information that was not known already. One could glean from the research that there are differences from system to system regarding how directors view website filtration. These differences are the basis behind the researcher's position to gain the understanding of legal interpretation behind CIPA and E-Rate. The interviews that were completed with the Professor, Auditor, and the E-Rate Specialist were to gain interpretation of legal issues that may effect the decision of technology directors.

Professor Interview. A professor who teaches actively in a university setting on educational law was interviewed about the Children's Internet Protection Act. "The Children's Internet Protection Act was passed to protect children from harmful materials on the Internet. It established regulations for E-Rate recipients to certify efforts to implement Internet safety measures in order to receive E-Rate funding" (personal communication, August 19th, 2010). This is the fundamental basis for the Children's

Internet Protection Act and justifies the enforcement of “harmful to minors” by school systems throughout the networks.

> “Harmful to minors” and “obscene” is any picture, image, graphic image file, or other visual depiction that (1) taken as a whole and with respect to minors, appeals to a prurient [erotic] interest in nudity, sex, or excretion; (2) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (3) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors (personal communication, August 19th, 2010).

When a website is taken as a whole and lacks the serious literary, artistic, political, or scientific value, it must pass the Miller Obscenity Test before being deemed inappropriate for minors. This test includes:

> (a) whether “the average person, applying contemporary community standards” would find that the work, taken as a whole, appeals to the prurient interest, [Roth, supra, at 489,]
>
> (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law, and
>
> (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value. If a state obscenity law is thus limited, First Amendment values are adequately protected by ultimate independent appellate review of constitutional claims when necessary” (Miller vs. California, 1973).

The requirements of the Children’s Internet Protection Act include an Internet Safety Policy and an Internet protection measure followed up by training to staff and students.

> Social Networking or websites such as YouTube is not considered a violation to CIPA. CIPA merely requires a safety policy, implementation, and training. If social networking, in any particular circumstance, clearly and significantly leads to safety threats, in violation of the system's policies, then there might be a basis for asserting a violation. Most of the determination as to what constitutes proper safety measures and implementation lies with the local decision-makers and administrators. I am not aware of any suit based, simply, on a district allowing social networking or related websites. This does not mean a system could not be liable for allowing or overlooking harmful social networking via the system's network, under some other law or legal principle such as Negligence. (personal communication, August 19th, 2010)

School systems are allowed to regulate networks as long as it regulates material reasonably.

> A school system is generally free to regulate its curricular resources, including Internet access, as long as it acts reasonably, consistently with its purpose of educating students in an orderly way, and is basing its decision on what is educationally suitable. Students, generally, don't have a right to use school-provided Internet resources however they want, although there are some limitations that future 1st Amendment litigation may address such as when schools over-restrict the Internet and prevent students from accessing legitimate information. (personal communication, August 19th, 2010)

Anyone who is an employee of the government has limited rights as to what they can access when they are using government owned equipment.

> Government employees, including teachers, have virtually no rights as they pertain to what they can access, at least in our jurisdiction. The 4th Circuit Court of Appeals who has jurisdiction in North Carolina in Urofsky v. Gilmore clearly ruled that university faculty members have no academic freedom that requires a government employer to provide any degree of Internet access. The reasoning is that the government owns the computers and network and, as the employer, has the complete right to regulate their use. (personal communication, August 19th, 2010)

While this is a case that was ruled for a university, it is usually implied that the case would pertain to a K-12 classroom. It is not the requirement of a school system to give reasons as to why a website is blocked.

> Technically in most circumstances, the school system probably wouldn't have to give reason unless due process rights were involved, but it needs to have reasonable reasons and be able to convince a court and document reason(s). If sued, the system would have to show that the decision is based on what school officials reasonably deem to be a reasonable, legitimate curricular and/or administrative basis. In practice, there should be a policy in place that, among other things, provides guidelines as to what will be allowed and prohibited, generally, plus it is good to establish a process for making determinations, allowing waivers, and addressing requests for reconsideration or exceptions. Furthermore, it is normally not good practice

> to issue decisions without providing some reasonable explanation when requested. (personal communication, August 19th, 2010)

Interpretation is key when discussing CIPA, but the bottom line is that until "local decision" is defined, the appointed party that makes the daily decisions regarding websites will have the final say. E-Rate requires school systems to purchase website filtration, and that it functions properly, but it does not require technology directors to block specific sites, other than pornography. States employ specialists to help LEAs understand the policies of E-Rate and what they must do to comply with those guidelines.

E-Rate specialist. "E-Rate is administered by the Universal Service Administrative Company (USAC) under the direction of the Federal Communication Commission, which provides discounts to assist most schools in the United States to obtain affordable telecommunications and Internet Access" (personal communication, July 1st, 2010). The funding provided by E-Rate is then controlled and investigated by USAC through an auditing process.

> The Federal Communications Commission (FCC) instructs USAC to contract with outside auditors such as KPMG, Grant Thornton and others to conduct a specific number of audits each year. USAC also has an internal audit division for special situations. Additionally, USAC occasionally asks school districts for proof of CIPA compliance during routine form review. (personal communication, July 1st, 2010)

When audits take place with a school system, the auditors will typically search to make sure the filter is turned on and that it is blocking appropriate pages. "If a district's Internet Safety Policy specifically addresses certain types of sites the auditor may check

to see if the content filter is doing what the policy says it is doing and interpretation could come into play" (personal communication, 2010). When asked if school systems could lose their funding for certain websites being available to students such as Facebook, YouTube, or Twitter the response was again directed to the AUP/Internet Safety Policy. "I would caution that it is possible to lose funding if the district has an Internet Safety Policy that specifically states that students will not have access to social networking sites" (personal communication, July 1st, 2010).

E-Rate does not make recommendations to technology directors because the wording of CIPA allows the LEA to promote local control of what is appropriate and what is not appropriate for their students. When asked how many school systems have lost their funding based on students having access to Facebook, YouTube, or Twitter the E-Rate specialist replied, "zero."

The E-Rate specialist shared information relating to the definition of Telecommunication and Information Services and how it applies to United States law. Telecommunications is defined as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received" as defined in [46 U.S.C. 153 (43)].

The E-Rate specialist shared information relating to the definition of Internet Access as an information service which is "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications" [47 U.S.C. 153 (20)] (personal communication, July 1st, 2010).

Auditor. The auditor has performed approximately sixty-seven audits and is currently employed with the Universal Services Administrative Company through the Internal Auditing Division. When school systems are audited, the auditor will search for a functioning Internet filter that complies with the rules of CIPA. "We attempt to verify that the applicant has a working technology protection measure in place at the time of the audit, and that a technology protection measure was in place during the time period that is being audited" (personal communication, September 16th, 2010). When searching for specific sites the auditor was unable to provide information citing the inability to divulge specific identifiable information. However, there are procedures that are used to obtain that the filter is working correctly.

> The FCC has not established any guidelines in order to determine if a website filter is not working appropriately, nor have any accuracy or efficiency guidelines been established. Because new websites are established everyday, we understand that there may be a time delay before it is recognized as a harmful website and is blocked by the technology protection measure. Therefore, we discuss the applicant's Internet Safety Policy and technology protection measure along with their policies and procedures to determine how updates to the list of blocked websites are made and how often those updates are made. (personal communication, September 16th, 2010)

Social networking and other sites such as Blogger and YouTube do occasionally come up in conversation with LEAs, but each LEA handles the topics differently. When speaking with USAC, information was relayed that the Internal Audit Division of USAC

does not pull funding based on the finding of auditors. Once the auditor has filed a report, then that information is forwarded to the Schools and Libraries Program management if a school system failed to have a "technology protection measure that protects against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of the computers by minors, harmful to minors" (personal communication, September 16th, 2010).

Discussion

Qualifications of Technology Directors

It is important to always have qualified individuals making decisions when in a position of authority. Technology directors have to make decisions regarding educational validity of a website on a daily basis, and for an individual to do this they should have the certifications and degree requirements to do so. Out of the twenty-one Technology directors that responded to the survey, seven (36%) had a degree that was based in the field of Instructional Technology. This is a major concern as educators become increasingly advanced in the field of technology within school systems. In order to develop 21st Century skills there must be a demand that students, teachers, faculties, and administrators be informed about technology that will increase students' skills with technology in a globally competitive environment. With an approach to technology that is underfunded and understaffed, stakeholders and administrators must be aware that technology needs assistance in order to comply with 21st Century standards. Sixty-four percent of the individuals who responded to the survey have degrees ranging from bachelors to an Ed.D., in fields unrelated to technology. To increase these percentages job descriptions should be updated to require that technology directors obtain or maintain a Master's Degree in the field of Instructional Technology to allow for improvement with allocation of funds and professional development.

When technology directors make relevant decisions for classroom content on a webpage, most of them are technically unqualified to appropriately make that decision since they lack technological educational requirements. Out of those who responded to the survey, 86% make the day-to-day decision. This means that the majority of those that

do not have a technology background actually make the decision regarding student access in schools.

Processes Used To Approve Websites

When technology directors are faced with the challenge of approving websites, they are usually given an appointment to do so from the school board or superintendent. This appointment is granted through the CIPA legislation and not much thought is given to the promotion or election of those people who make the decisions. What the technology directors choose to do with this responsibility is left to their discretion since CIPA creates the "local decision" clause when implementing the law to minors. Some technology directors are bypassed completely and the director of the network is given the ability to determine if a website is viewable. Most of these individuals retain a Bachelor's Degree or an Associate's Degree to fill this position resulting in inadequate qualifications to determine educational value. Having an appropriate and certified educational background is essential for relevant interpretation of CIPA regarding usage of website filters to teachers. Technology directors maintain the ability to approve or disallow websites from ever getting to the student's computer. However, there are no guidelines or rules to follow other than that of what CIPA requires. Thus, how do technology directors decide what is educational in value or not? When researching the wording of CIPA the first two clauses speak specifically of pornography and graphic material, while the third part of the law is related to the validity of a website based on the literary, artistic, political, or scientific value as it relates to minors. Furthermore, adults can circumvent the filters enacted by schools to perform bona fide research as it relates to education.

In most districts, the technology directors are the sole representatives determining the validity of websites as it pertains to students. When individuals in these positions decide a website is inappropriate, is their determination based upon personal beliefs of what they consider to be educational or based upon the local community's thoughts on education? Technology directors should encounter a webpage objectively, without personal interest, and decide if the website in question interferes with CIPA or with local standards. Based on the interview with the professor, the CIPA clause that discusses the "literary, artistic, political or scientific values" was written so that whoever made the "local decision" could not prevent webpage access due to individual biases, but rather, based on a serious lack of educational value.

E-Rate is what provides most school systems the funding needed to maintain Internet access in the public school system. With E-Rate, technology directors are given five steps to protect students from websites that could be harmful to them through the use of "inappropriate matter." These five steps are included in a school system's Internet Safety Policy and include but are not limited to inappropriate matter, safety and security of minors, hacking, disclosure of personal information, and measures to restrict access (filters) to minors. If the Internet Safety Policy has been agreed upon and a subsequent violation occurs, the administration should hold teachers accountable for failing to monitor students when accessing a computer. In light of accountability, the student should also be held responsible for his/her actions when using the Internet at school. Administrators should trust teachers enough to allow access to material that could in fact be a teacher driven instructional resource.

Some technology directors, depending on the type of networks they run, do allow teachers access to Facebook, YouTube, and Twitter. Teachers are allowed to access these sites because the full filter has been applied to student networks, but the teacher network has a limited filter through tiered access. This sets the stage across districts for equal Internet but unequal content between teacher and student availability to enrich education. When one school system allows access of a website to teachers so they can be the driver of instruction, while a neighboring school system opposes that type of instruction, it raises the question of why one system felt the "local decision" needed to be invoked while the other did not. How can the state of North Carolina effectively say that students are receiving a level education when available resources are being withheld by local administrators? Students may not receive the same text books from district to district; however, the text book still has to follow the guidelines set by the Department of Public Instruction. Often, departments have vertical curriculums that link to YouTube or other websites to which teachers do not have access. How can teachers be held accountable for lower scores when a school system does not allow them access to tools that could enhance instruction?

Tiered access provides a viable solution to the "all or none" approach most school systems use in an otherwise complicated process of what is and is not appropriate. A teacher should have the freedom to bring in whatever resources he/she can to make instruction relevant to students as long as it is educational and complies with the law. While working within the confines of the law is important, school systems should not go beyond the intention of the law when disallowing websites from being accessed. A few technology directors address these issues by allowing for a committee process for website

approval in the system. A committee of administrators, principals, and teachers can enforce the “local decision,” and the technology director does not need to invoke authority on the mass of students they work for everyday unless a direct security issue arises for students or staff.

Educational Value

When comparing questions posed to technology directors, disparate results were found between questions regarding thoughts on educational websites and which of those websites were actually available. Twitter, for example, had a 47% approval, 24% neutral, and a 29% dislike of the website; Twitter was blocked by 52% of the schools surveyed. When comparing statistics, those claiming dislike and neutral were close to the actual denial of the website. Flickr’s results were 38% agree, 24% disagree, and 38% neutral. Flickr is open in 38% of the schools and blocked in 62%. It was interesting to find that those school systems who currently block Flickr were also 62%. Based upon these findings, an argument can be made that technology directors truly make a local decision and put the protection of students first above the educational value of the website. However, with the data presented for both Twitter and Flickr, the argument could also be made that technology directors make decisions without determining if a website is truly educational. With the percentage of directors who chose to be neutral on key websites, as suggested in Table 1, it may be in their best interest to utilize a committee for determining the validity of a webpage through consensus. The decision of a committee would be democratic and gain less of a reaction than one person making the decision in a dictatorship.

Congress placed the "local decision" clause in the CIPA, which allows the school board or superintendent to appoint the right person to do the job. This is most likely the technology director because the decisions are technology based. The technology director can decide without any oversight as to what is really educational or not, but there is uncertainty to the intention of the law as viewed in this manner. How can school systems block a site like Flickr, which contains art and photography? How does this website fit into the third clause of CIPA, where taken as a whole, it lacks the serious literary, artistic, political, or scientific value as it relates to minors? Certainly a student could go on the website and search for terms like "nude" or "sex," but where are the teachers when this is occurring? Where is the accountability of the teachers and students when students try to access harmful material? The Internet Safety Policy deemed necessary by E-Rate should be enough to deter content from being searched. The Internet Safety Policy states what will happen to faculty and students if they misuse the Internet or network. Why is their punishment for violating these policies not enough that the whole community has to suffer? Why are the filters that these districts purchase not blocking against specific material on a page instead of an entire domain?

When technology directors utilize the "local decision," educators may lose the ability to use real world connections. If technology directors would trust teachers to manage their classrooms and create guidelines for the state, all students in the state would have more tools available to them to succeed with end-of-year testing. When a school system has the authority to block material from the Department of Public Instruction regarding curriculum, that school system may be doing a disservice to the community. School systems deny access by protecting students through doctrines such as "*in loco*

parentis," but the system may inhibit the student's ability to be a globally competitive citizen in today's 21st Century classroom.

Technology directors

Technology directors are usually given authority through a school board or the superintendent to provide Internet access to students. This access, through E-Rate funding, requires school systems to purchase and maintain a filter to protect students from inappropriate matter. Most technology directors do not have a choice over the type of filter previously purchased. However, technology directors can create a vision of positive filter usage so teachers and students can both excel. An all or nothing approach is inappropriate in the digital age. Educators should try to protect students but should provide teachers with maximal resources available to enable teacher driven instruction, thereby increasing students classroom skills and progress.

Websites should not be blocked unless these sites are a direct violation of CIPA or pose a security concern among the students. If teachers complain students are "on Facebook too long" as noted in one of the technology director interviews, then teachers may need to be coached with techniques on how to effectively manage their classroom. Teachers should have enough authority in the classroom to manage computer usage preventing technology directors from blocking websites due to a lack of trust. Neither technology tools nor faculty in a school district should be penalized simply because one teacher cannot manage his/her class.

Most technology directors wish to protect students and are legally allowed because of *"in loco parentis."* School boards empower technology directors with the ability to invoke a "local decision." At what cost are students' educations hampered by

following current practices? The local decision should be transformed from a one person solution to a multi-person collaboration through the use of a committee or representative panel. This committee could look different based on the make-up of a school system. As a suggestion to effectively reach a "local decision" in a school system, one person at each school should be part of a committee in order to reach a consensus for website approval. How can one technology director who may not even live in the county or system of employment be the effective "local decision"? How are political and personal issues eliminated when websites are blocked? Why is CIPA or negligence not being cited when school systems continue to block sites in order to provide transparency to these policies and laws? Teachers would be more understanding if they were given a time frame for when a request to unblock a website would be reviewed. Furthermore, a vote count and anonymous recommendations from representatives should be part of the process. Teachers should receive an explanation of parts of the law or Internet Safety Policy that the website violates if it remains blocked.

Access to the Internet by teachers is a driving point as to what type of education students can receive in the classroom. Some school systems have a tiered access through the network that permits teachers and students to access the Internet in different ways. Teachers can have access to YouTube, Facebook, and Twitter while utilizing them from an educational perspective when demonstrating topics in the classroom setting. Some of those tools are not the best for students because of safety concerns, but when driven by the teacher many sound and useful practices can result. Under a tiered network, teachers would be able to have the Internet to research information possibly needed for instruction.

Some school systems allow the teacher network on personal wireless devices. Others will have set up usernames on the system to allow for access to be granted based on login information. Even still there are many systems that have an all or nothing approach when allowing teachers and students access. The balance of technology in school systems is affected when there are other options for teachers to obtain tools that they can not use due to ineffective networks. Until the Department of Public Instruction or a group of technology directors create a uniform process of developing a vision of technology standards and guidelines in schools, students could suffer and may not have a level playing field for end-of-year testing and assessments as it relates to Internet use.

Professor

The professor cleared up many issues concerning CIPA and what school systems must implement as long as students have access to the Internet. Regardless of whatever program may be in place from the federal government, all schools must protect students from harmful materials on the Internet. With the creation of E-Rate, the government decided to pay for most of the funding required by school systems to afford Internet access. When a school system receives money from E-Rate, that school system must create and approve an Internet Safety Policy with appropriate measures to protect students from harmful materials. In order for a website to be blocked, the website must pass the Miller Obscenity Test. When a website is blocked and fails to meet the requirements of the Miller test, that website should be unblocked unless it creates a security concern for students. In regards to Facebook, a technology director does not really have the right to block the site as it relates to minors based on the Miller Test.

However, negligence laws and safety concerns could allow that school system to block the website due to the nature of some of the site's programs and abilities.

The fact that students must be above the age of thirteen to use Facebook is by far enough to consider the website inappropriate for minors based on other laws such as the Children's Online Privacy Protection Act. If the network was set up in such a way that age could be differentiated based on high school, middle school, and elementary school, perhaps Facebook may have a place with students at the high school level. If a school system would enact a tiered website filtration system, the network related to teachers would have more leniencies because that network is for adults only. Meanwhile, the students would have more websites such as Facebook blocked because negligence and security concerns would be an issue.

In contrast, school systems always retain the right to use and secure the network as needed. Teachers are not given any rights as to what they can access in the classrooms regardless of needed research. CIPA is written so that teachers can have access to websites around the filter due to "bona fide" research, but then the government sets limits to this interpretation of the law by ruling against it in the case of Urovsky vs. Gilmore in the 4th Circuit Appeals Court. To put the decision in context, this is a "law restricting state employees from accessing sexually explicit material on computers that are owned or leased by the state" (Urofsky vs. Gilmore, 1999). Even with the limitation to what teachers can access, they are still able to access material that is educational in value as it relates to curriculum. Most teachers who submit requests to have websites opened are not going to use websites unsuitable for minors.

E-Rate Specialist

The E-Rate specialist confirmed that E-Rate is the controlling body of funds to school systems regarding Internet access and telecommunications services. By giving funds to the school systems, E-Rate can also remove funding depending on the compliance of rules issued. When government funding is used on a wide basis, typically the government chooses to audit allocations of their funds. Auditors will check the school's books and equipment to be sure the funding received is being used correctly. By doing this, auditors may go to a computer and access the Internet to make sure appropriate websites or something specifically mentioned in the Internet Safety Policy is being protected against.

The purpose of filters purchased by school systems are to enforce the tenets of the law. CIPA is related to visual graphics that are obscene, harmful to minors, or hold no educational value. E-Rate encompasses this law to include inappropriate matter not suitable to minors. The Internet Safety Policy is the basis for what auditors research when they enter a school system. While all school systems mention limitations to student use on the Internet, to date no school system has ever lost funding due to websites being available such as Facebook, Twitter, or YouTube. E-Rate is usually the agency that takes the brunt of the blame from technology directors when citing reasons for blocking a website. Whether systems want to cite negligence or safety concerns, they need to accept that responsibility and communicate correct information to staff and students. Teachers should not be informed that E-Rate is the driving force behind what students can learn in the classroom when in reality the "local decision" applies, and the school system is the

main body rejecting websites. E-Rate enforces CIPA but does not regulate the day to day resources students use.

E-Rate Auditor

The auditor's main goal when investigating a school system as it relates to websites is to assure that system has an Internet protection measure and policy in place during the time period for which it is being audited. With no guidelines established by the FCC the auditors look at websites that should be blocked while recognizing that there are delays in the updates of the blocked lists. When auditors visit a school system, their duties extend to all areas that E-Rate has funded and is not directly related to the Internet filter; however, the Internet filter is a component of investigations.

It is important to recognize that these auditors do not have guidelines set by the FCC and are completely reliant on the wording of CIPA and the wording of each individual school system's Internet Safety Policy. The standard is set for the "local decision" to be the main determination of what students have access to in the classroom. Under this guise technology directors are the focal point of what students can be given access to in terms of educational value. One technology director per school system with one hundred and fifteen different districts all implementing technology differently while all of our students take the same type of test at the end of the year is unacceptable.

Conclusions and Future Study

Conclusions. Parents, teachers, students, and all others affected by the current education system should be aware of the manner in which technology is implemented in the 21st Century classroom. An era of collaboration, global competitiveness, and constant skill acquisition is being uprooted by barriers that could be prevented. These barriers

hinder a student's ability to reach websites that could enhance learning in an everyday setting beyond the classroom. CIPA and E-Rate protect students from obscene matter but the "local decision" implemented by technology directors, as stated by the professor, could be over-restricting access to teachers. It is important to note that authority to restrict Internet access to minors is top priority when in a public school setting, but it is time that teachers are given separate rights from students in order to drive instruction. Technology directors who have been appointed by school boards or superintendents have the final decision, but those entities should review the processes of how that decision is determined.

A new model must be implemented and technology directors need to become a unified front when deciding upon Internet access to students and staff. Access is important, and not only should technology directors be unified, but should also take into account the voices and concerns of teachers and students. This new model should include all or some of these components:

- The state of North Carolina should recommend that technology directors meet annually as a region to develop a set of guidelines for blocking websites and discussing new networking options.
- The regional set of guidelines formed should be aligned with other regional guidelines within the state of North Carolina to create an optional state standard of guidelines.
- When a state standard of guidelines has been established technology directors should put forth effort to comply and better their school districts based on those guidelines to create a uniformed approach to Internet access throughout the state.
- School districts should implement a tiered network to allow students at elementary, middle, and high to have separate access levels while allowing teachers the ability to drive instruction on their own network. Access to websites should be limited to teachers per the wording of CIPA as it relates to the United States Constitution and 1st Amendment rights. Access to social networking, video networks, and other non-pornographic websites should be allowed as a teacher

driven resource. Teachers should have the opportunity to research and implement websites into curriculum without the approval of the technology director. Before students can access websites that are blocked on their networks, then that website must pass a representative majority. Teachers should be held accountable when the Internet Safety Policy is not followed.

- Technology directors should not be the sole decision in determining what can be unblocked without representative approval. However, they should be able to determine what should be blocked as it relates to the literal reading of CIPA and the Internet Safety Policy as long as it does not infringe on the wording of CIPA. Websites to be unblocked should go through an approval committee. The committee make up could vary but it should have individuals from different departments including teachers and staff whose tenure changes yearly and does not repeat to allow for appropriate consensus. The ideal setting for a committee would be to include one representative from each school to effectively determine the "local decision." When representatives are asked to respond they should have the wording of CIPA readily available as a guideline to establish an appropriate "local decision." This can be anyone who is certified in the school and the individual in this position should change on a yearly basis. This should be done weekly, bi-weekly, or monthly but no more than a month should pass. A survey with "yes" or "no" could be established with the option of "no" requiring reasoning. A simple majority of 51% should suffice for approval. Results should be sent district wide to allow teachers the opportunity to see what websites have recently been opened or denied.

- As requests for websites to be unblocked are received the technology director should build a table or survey with a clickable url of the website and a section to vote "yes" or "no" with a reason for voting "no" as a requirement. The reasoning is important because representatives should use the wording of CIPA and the Internet Safety Policy to determine the validity of a webpage for teacher access. The technology director would still retain the right to block access to pages based on other policies set by the school board.

- The school district should be notified by the technology director as to why websites are not allowed to be unblocked citing reasons such as CIPA, Internet Safety Policy, or negligence with that portion of the law or policy attached. The results from the survey should also be attached allowing for transparency of the process.

- As an option to refute the blocking or unblocking of a website after representative review, teachers, students, and parents should have an outlet to voice their opinions and submit proposals to have websites reviewed on a case by case basis as to their validity of educational value. These reviews can be handled internally through the technology department of each system.

Technology directors perform well with the resources available but reform needs to occur in order to better benefit students in a 21st Century classroom. As society progresses and becomes more engrained with social networking and emerging technology devices it will only become increasingly difficult for technology directors to maintain the needs of the network, school, students, staff, or administrators. Students should have equal opportunities when it comes to Internet access across the state. To do this school systems need to incorporate a filter that will allow for varying Internet access levels for elementary, middle, high school, and teacher networks. Websites that the North Carolina Department of Public Instruction use should not be blocked from access to students or faculty because of the medium they use to inform school systems. The Internet is not free, but several of the districts in North Carolina have close to one hundred percent connectivity (Appendix I: state connectivity). Why then are technology directors only allowing students to barely touch the potential that is in the world through the Internet by limiting teacher resources? There are many barriers that affect how students are able to utilize technology within educational experiences. Technology directors should not be a barrier but an open door for students to reach full potential.

Problems and Limitations. A number of problems and limitations presented while the research was conducted and interpreted. A problem that commonly asserted itself was the lack of response to the survey. One hundred and fifteen school systems were contacted to participate in the survey. Twenty-one responded to the survey which was well under the projected amount of a fifty percent return. The more results given would have allowed the researcher to obtain a baseline significant enough to show the variance of technology director decisions and ideas from across the state. However, there

are pockets of data collected that represent the four main geographic regions of North Carolina. The responses obtained from the sample were varied enough to represent the population as a whole.

In Table 1, the survey did not differentiate between student access and teacher access when asked about specific websites being available. This was a factor that could have hindered results because the technology director would be unable to interpret correctly if the question asked was meant for the school district, teacher, or student. The opinions of the results in the table could have changed if the director was able to interpret teacher driven websites versus non teacher driven websites. This limitation would need to be addressed if the study were to be performed again. The education level given by directors is misleading for those that responded with the Ed.D as their choice of education. The problem with this choice is that the researcher cannot ascertain if the director actually had a background in instructional technology or a background in administration.

Technology director interviews were only from a specific region in the state and not from several regions. This limits the researcher from establishing the connections of a multi-region-based local decision. It was not possible for the researcher, due to time constraints, to interview technology directors from all regions. The researcher considered the best approach was to ascertain interviews completed with neighboring school districts to show the variance of the “local decision” and access as it relates to a specific region within the state. Therefore, the information gathered from this region may not be representative of the state as a whole.

Future Research. Future research based from this study would be interesting if a region in North Carolina would be willing to create a set of networking and website guidelines that would enforce rules, set standards, and collaboratively reach a local decision on website access to teachers and students. This group would maintain the same website filtration list and implement the same Internet Safety Policy. The data collected could then be correlated with end-of-year testing growth based on this region's results compared to another region's results that have varying Internet access and networking levels. The school systems that are in the experimental group would develop a process to allow websites and to provide feedback when websites are not approved. The overall idea is to research positive growth on end-of-year testing which could be a result of students and teachers gaining access to materials that do not infringe on the tenets of CIPA or E-Rate. By creating a democratic and representative process for website approval, school systems may benefit from increased growth on end-of-year testing.

References

Ayre, Lori Bowen. (May 2001). *Internet Filtering Options Analysis: An interim report*. InFoPeople Project. http://statelibrary.dcr.state.nc.us/hottopic/cipa/InternetFilter_Rev1.pdf (Accessed 05/20/10).

Bertot, J. C. (2000). Universal service in the networked environment: The education rate (E-Rate) debate. *The Journal of Academic Librarianship, 26*(1), 45-48.

Federal Communications Commission. (2010). *Children's Internet Protection Act*. (2010, May 16). Retrieved from http://www.fcc.gov/cgb/consumerfacts/cipa.html

Houghton-Jan, S. (2008). *Internet filtering software tests: Barracuda, cyberpatrol, filtergate, & websense*. San Jose, CA: San Jose Public Library. Retrieved from http://www.sjlibrary.org/about/sjpl/commission/agen0208_report.pdf

McCarthy, Martha M. (2004). Filtering the Internet: The Children's Internet Protection Act. *Educational Horizons*, 82(2), 108-113.

Miller vs. California, 413 U.S. 15 (1973).

Offenses Against Public Morals §19, NCGS, §1.1, (2010).

Phelps, Shirelle, & Lehman, Jeffrey. (2005). In Loco Parentis. (2005). *West's Encyclopedia of American Law*. Detroit: Gale.

Park, Euna, Hansa, Sinha, & Jing, Chong. (2007). Beyond access: An analysis of the influence of the E-Rate program in bridging the digital divide in American schools. *Journal of Information Technology Education, 6*, 387-406.

Sexual Exploitation and Other Abuse of Children §110, 18 U.S.C. §2256 (465-466) (2010).

Universal Services Administrative Company. (2010, March 22). *Step 10: Children's Internet protection act*. Retrieved from http://www.usac.org/sl/applicants/step10/cipa.aspx

Urofsky vs. Gilmore, 167 F.3d 191 (4th Cir. 1999).

Wire or Radio Communication §5, 47 U.S.C, §254 (87-90), (2010).

Appendix A

Alan Warren - IRB Notice

From: IRB <irb@appstate.edu>
To: <aw78071@appstate.edu>
Date: 6/28/2010 11:04 AM
Subject: IRB Notice

To: Alan Warren
College Of Education (dr. Charles Duke) ,
CAMPUS MAIL

From: _____
Julie Taubman, IRB Administrator

Date: 6/28/2010

RE: Determination that Research or Research-Like Activity does not require IRB Approval

Study #: 10-0269
Study Title: Web Filtering: An Evaluation of Local Education Agencies

This submission was reviewed by the IRB. It was determined that it does not constitute human subjects research as defined under federal regulations [45 CFR 46.102 (d or f)] and does not require IRB approval. If your study protocol changes, this determination may no longer apply, and you should contact the IRB before making the changes.

Appendix B – G (School System AUPs)

Appendix B

School #1 Student Required Use Policy, Board approved 8-11-09
Reference: PL §106-554
SCHOOL #1
STUDENT REQUIRED USE AND INTERNET SAFETY POLICY (RUP)
(in accordance with Children's Internet Protection Act [CIPA]
and North Carolina Public Law 106-554)

PURPOSE: School #1 provides all students access to the Internet, network resources as well as laptop computers at designated graded levels, as a means to promote achievement and provide diverse opportunities during the educational experience. This policy provides guidelines and information about the limitations that the school imposes on use of these resources. In addition to this policy, the use of any school computer, including laptop computers, also requires students to abide by the SCHOOL #1 Technology Use Guidelines as stated in the Student Code of Conduct. Additional rules may be added as necessary and will become a part of this policy.

TERMS OF THE REQUIRED USE AND INTERNET SAFETY POLICY
Specifically, the student: Will adhere to these guidelines each time the Internet is used at home and school.

- Will make available for inspection by an administrator or teacher upon request any messages or files sent or received at any Internet location. Files stored and information accessed, downloaded or transferred on district-owned technology are not private.
- Will use appropriate language in all communications avoiding profanity, obscenity and offensive or inflammatory speech. Cyber Bullying such as personal attacks and/or threats on/against anyone made while using district owned technology to access the Internet or local school networks are to be reported to responsible school personnel. Rules of netiquette should be followed conducting oneself in a responsible, ethical and polite manner.
- Will follow copyright laws and should only download/import music or other files to a district owned technology that he/she is authorized or legally permitted to reproduce, or for which he/she has the copyright.
- Will never reveal identifying information, files or communications to others through email or post to the Internet.
- Will not attempt access to networks and other technologies beyond the point of authorized access. This includes attempts to use another person's account and/or password.
- Will not share passwords or attempt to discover passwords. Sharing a password could make you liable if problems arise with its use and subject to disciplinary action.
- Will not download and/or install any programs, files, or games from the Internet or other sources onto any district owned technology. This includes the intentional introduction of computer viruses and other malicious software.
- Will not tamper with computer hardware or software, unauthorized entry into computers, and vandalism or destruction of the computer or computer files. Damage to computers may result in felony criminal charges.
- Will not attempt to override, bypass or otherwise change the Internet filtering software or other network configurations.
- Will use technology for school-related purposes only during the instructional day while refraining from use related to commercial, political or other private purposes.
- Will not make use of materials or attempt to locate materials that are unacceptable in a school setting. This includes, but is not limited to pornographic, obscene, graphically violent, or vulgar images, sounds, music, language, video or other materials. The criteria for acceptability is demonstrated in the types of material made available to students by administrators, teachers, and the school media center. Specifically, all district owned technologies should be free at all times of any pornographic, obscene, graphically violent, or vulgar images, sounds, music, language, video or other materials (files).

- Will not connect any personal technologies such as laptops and workstations, wireless access points and routers, printers, etc to district owned and maintained local, wide or metro area network. Connection of personal devices such as iPods, smartpphones, PDAs and printers is permitted but not supported by SCHOOL #1 technical staff. Home Internet use and cost is the responsibility of the student both in cost and configuration. Dial-up is not an option as recent laptop configurations do not include modems.
- Will keep laptop secure and damage free. Each laptop is issued with a protective book bag style case. Use of provided laptop bags is required at all times. Follow these general guidelines:

- Do not loan your laptop or charger and cords.
- Do not leave the laptop in vehicle.
- Do not leave your laptop unattended.
- Do not eat or drink while using the laptop or have food or drinks in close proximity to the laptop.
- Do not allow pets near your laptop.
- Do not place the laptop in floor or in sitting area such as couches or chairs.
- Do not leave the laptop near table or desk edges.
- Do not stack objects on top of your laptop.
- Do not leave the laptop outside or use near water such as a pool.
- Do not check the laptop as luggage at the airport.

- Will back up data and other important files regularly. SCHOOL #1 will at times maintenance the laptops by imaging. All files not backed up to server storage space or other storage media will be deleted during these processes. Students are ultimately responsible for backing up all personal files on their own storage media.

By signing this you agree to abide by the conditions listed above and assume responsibility for the care and proper use of SCHOOL #1 technology, including personally backing up personal data. SCHOOL #1 is not responsible for any loss resulting from delays, non-deliveries, missed deliveries, lost data, or service interruptions caused by user errors, omissions or reasons beyond the district's control. Information obtained via the Internet and other sources using SCHOOL #1 technologies is not guaranteed as to its accuracy or quality. I understand that should I fail to honor all the terms of this Policy, future Internet and other electronic media accessibility may be denied. Furthermore, I may be subject to disciplinary action outlined in the SCHOOL #1 Student Code of Conduct and, if applicable, my Laptop computer may be recalled. By signing below, I give permission for the school to allow my son or daughter to have access to the Internet under the conditions set forth above.

As the parent/guardian, my signature indicates I have read and understand this Required Use Policy, and give my permission for my child to have access to the described electronic resources.

Parent/Guardian (please print): _____

Parent/Guardian Signature: _____Date: _____

As the student, my signature indicates I have read or had explained to me and understand this Required Use Policy, and accept responsibility for abiding by the terms and conditions outlined and using these resources for educational purposes.

Student (please print): _____

Student Signature: _____Date:_____
Terms and Conditions: This RUP is valid through June 30, 2010

Appendix C

School #2 Technology Acceptable Use Policy
Board Policy 7320

Technological resources, including computers, other electronic devices, programs, networks and the Internet provide opportunities to enhance instruction, appeal to different learning styles, and meet the educational goals of the board. Through the school system's technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects and acquire access to current and in-depth information.

Use of technological resources should be integrated into the educational program. Technological resources should be used in teaching the North Carolina Standard Course of Study and in meeting the educational goals of the board. The curriculum committee should provide suggestions for using technological resources in the curriculum guides as provided in policy 3115, Curriculum and Instructional Guides. Teachers are encouraged to further incorporate the use of technological resources into their lesson plans.

The superintendent shall ensure that school system computers with Internet access comply with federal requirements regarding filtering software, Internet monitoring and Internet safety policies. The superintendent shall develop any regulations and submit any certifications necessary to meet such requirements.

A. REQUIREMENTS FOR USE OF TECHNOLOGICAL RESOURCES

The use of school system technological resources, such as computers and other electronic devices, networks and the Internet, is a privilege, not a right. Before using the Internet, all students must be trained about appropriate on-line behavior. Such training must cover topics such as cyber-bullying and interacting with others on social networking websites and in chat rooms.

Anyone who uses school system computers or electronic devices or who accesses the school network or Internet, at an educational site, must comply with the requirements listed below. All students and employees must receive a copy of this policy annually.

Before using school system technological resources, students and employees must sign a statement indicating that they understand and will strictly comply with these requirements. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges. Willful misuses may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

1. School system technological resources are provided for school-related purposes only. Acceptable use of such technological resources are limited to activities that support learning and teaching. Use of school system technological resources for commercial gain or profit is prohibited.

2. Under no circumstance may software purchased by the school system be copied for personal use.

3. Students and employees must comply with all applicable board policies, administrative regulations and school standards and rules in using technological resources. All applicable laws, including those relating to copyrights and School #2 Technology Acceptable Use Policy Board Policy 7320 trademarks, confidential information and public records, apply to technological resource use. Any use that violates state or federal law is strictly prohibited.

4. No user of technological resources , including a person sending or receiving electronic communications, may engage in creating, intentionally accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing or considered to be harmful to minors.

5. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).

6. Users must respect the privacy of others. When using email, chat rooms, blogs or other forms of electronic communication, students must not reveal personally identifiable, private or confidential information, such as the home address or telephone number, of themselves or fellow students. In addition, school employees must not disclose on the Internet or on school system web sites/pages any personally identifiable information concerning students (including names, addresses or pictures) without the written permission of a parent/guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or policy 4700, Student Records. Users also may not forward or post personal communications without the author’s prior consent.

7. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software or computer networks. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses.

8. Users may not create or introduce games, network communications programs or any foreign program or software onto any school system computer, electronic device or network without the express permission of the technology director or designee.

9. Users are prohibited from engaging in unauthorized or unlawful activities such as “hacking” or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.

10. Users are prohibited from using another individual's computer account. Users may not read, alter, change, execute or delete files belonging to another user without the owner's express prior permission.

11. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the School #2 Technology Acceptable Use Policy Board Policy 7320 problem to other users. Any user identified as a security risk will be denied access.

12. Teachers shall make reasonable efforts to supervise a student's use of the Internet during instructional time.

13. Views may be expressed as representing the view of the school system or part of the school system only with prior approval by the superintendent or designee.

B. Restricted Material on the Internet

Before a student may use the Internet for any purpose, the student's parent must be made aware of the possibility that the student could obtain access to inappropriate material. The parent and student must sign a consent form acknowledging that the student user is responsible for appropriate use of the Internet and consenting monitoring by school system personnel of the student's e-mail communication and use of the Internet. The board is aware that there is information on the Internet that is not related to the educational program.

The board also is aware that the Internet may provide information and opportunities to communicate on subjects that are not suitable for school-age children and that many parents would find objectionable. School system personnel shall take reasonable precautions to prevent students from having access to inappropriate materials, such as violence, nudity, obscenity or graphic language which does not serve a legitimate pedagogical purpose. The superintendent shall ensure that the Internet service provider or technology personnel has installed a technology protection measure that blocks or filters Internet access to audio or visual depictions that are obscene, that are considered pornography or that are harmful to minors. School official may disable such filters for an adult who uses a school-owned computer for bona fide research or another lawful educational purpose. School system may not restrict Internet access to ideas, perspectives or viewpoints if the restriction is motivated solely by disapproval of the ideas involved.

C. PRIVACY

No right of privacy exists in the use of technological resources. School system administrators or individuals designated by the superintendent may review files, monitor all communication, and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School system personnel shall monitor on-line activities of individuals who access the Internet via a school-owned computer.

D. PERSONAL WEBSITES
The superintendent may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize school system or individual school names, logos or trademarks without permission.

School #2 Technology Acceptable Use Policy Board Policy 7320

1. Students
Though school personnel generally do not monitor students' Internet activity conducted on non-school system computers during non-school hours, when the student's on-line behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy (see the student behavior policies in the 4300 series).

2. Employees
All employees must use the school system network when communicating with students about any school-related matters. Thus, employees may not use personal websites or on-line networking profiles to post information in an attempt to communicate with students about school-related matters. Employees are to maintain an appropriate relationship with students at all times. Employees are encouraged to block students from viewing personal information on employee personal websites or on-line networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. If an employee creates and/or posts inappropriate content on a website or profile and it has a negative impact on the employee's ability to perform his or her job as it relates to working with students, the employee will be subject to discipline up to and including dismissal. This section applies to all employees, volunteers and student teachers working in the school system.

School #2 Technology Acceptable Use Policy
Board Policy 7320
Employee Agreement:
I understand and will abide by the above Rules and Regulations for School #2 Networks. I further understand that any violation will result in the loss of access privileges and disciplinary action.

Employee Name (Please Print): _____

Employee Signature: _____ Date: _____

Appendix D

School #3 Employee Acceptable Use Policy

Reference: North Carolina Public Law §106-554

General Purpose and Use

The Internet connects computers and computer networks worldwide, creating access and links to an infinite number of resources and individuals. School #3 is committed to the use of electronic resources and technology to enhance the administrative, teaching and learning opportunities for students, administrators, faculty, and staff. Internet use is increasingly fundamental for students and employees to be able to electronically communicate with others, and to obtain and transmit diverse types of valuable, educational information. In continued pursuit of educational excellence, students and employees in all schools and sites have available Internet access. However, users must bear in mind that access and use of Internet and electronic communication is considered a privilege and not a right. Misuse of these resources may result in loss of this privilege, as well as possible disciplinary and/or legal action.

Guidelines and Responsibilities

Employees will:

- Recognize that Internet access is available to SCHOOL #3 employees for educational and work related purposes only.
- Comply with copyright laws, federal, state and local laws prohibiting obscene or profane language or material, and local school system rules and regulations regarding types of material and usage.
- Recognize that the school system may monitor access to computer resources to ensure security and performance of computer systems and networks, to review employee performance, and to enforce applicable laws and policies.
- Supervise and facilitate student use of technology.
- Model and provide instruction in the ethical and appropriate use of technology in a school setting.
- Ensure all student users have a signed Student Acceptable Use Policy before allowing them to access the Internet.
- Use assigned account, ID, or password only, not sharing with any other employee or student.
- Keep user ID’s, passwords, and computer resources secure.
- Refrain from activities that could disrupt network functions.
- Refrain from the install, download or copy of any software, or files without permission from district technology personnel.
- Avoid the intentional access, production, posting, sending, displaying, and or retrieving sexually explicit, vulgar, obscene, offensive, or otherwise inappropriate materials.

- Care for computer equipment and network resources causing no damage or intentional unauthorized changes.

School #3 Employee Acceptable Use Policy

Reference: PL §106-554 March 6, 2006
Page 1 of 2

- Attempt no unauthorized access into any network, system, program or account.
- Access chat rooms, e-mail, list-servs, or other electronic communication methods for educational and work related purposes only.
- Reveal personal information across the Internet cautiously.
- Report inappropriate use of the network or security problems to technology personnel.
- Understand that files stored on school system servers and workstations will not be guaranteed to be private or secure.
- Not use school system electronic mail inappropriately by:
- Sending email that is intimidating or harassing.
- Using email for personal business, political lobbying or campaigning.
- Sending or forwarding chain emails to individuals or groups.
- Creating or transmitting email or images that might be considered inappropriate in the workplace, including, but not limited to, messages or images that are lewd, obscene, sexually explicit, pornographic, harassing or offensive.
- Using email for commercial or solicitation purposes.
- Sending mass emails using school system email for any purpose except those relating directly to instruction and school administration.
- Sending mail that may be considering harassing, threatening or an attack on individuals or groups.
- Forward voicemail to email/wav files without proper permission forwarding only to appropriate SCHOOL #3 staff for further facilitation.

Security and Disclaimer

The School #3 utilizes software that attempts to prohibit access to information and Internet sites considered obscene and/or harmful. However, employees may either purposefully or inadvertently encounter material or information not intended for educational purposes. Electronic mail (email) is not guaranteed to be private and may be monitored, mis-delivered or read by others. However, appropriate and positive use of this resource and the Internet ultimately remains the responsibility of the user. Therefore, the School #3 is not responsible for damages or losses suffered during Internet and email use and access. This includes, but is not limited to, loss of or corrupted data, service interruptions or delays, or obtaining information of poor quality, containing errors, omissions or inaccuracies, or material of questionable or harmful value in either type or intent.

As an employee of the School #3, my signature indicates I have read and understand this *Policy for Acceptable Us*e, and accept responsibility for abiding by the terms and conditions outlined and using these resources for educational purposes. I also acknowledge that I have read and understand the contents of the *General Network Security Policy*.

Employee (please print): _____

School/Location: _____

Employee Signature: _____ Date: _____

Appendix E

Policy Code: 3225/7320 Technology Acceptable Use
Technological resources, including computers, other electronic devices, programs, networks and the Internet, provide opportunities to enhance instruction, appeal to different learning styles and meet the educational goals of the board. Through the school system's technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information.

Use of technological resources should be integrated into the educational program. Technological resources should be used in teaching the North Carolina Standard Course of Study and in meeting the educational goals of the board. The curriculum committee should provide suggestions for using technological resources in the curriculum guides as provided in policy 3115, Curriculum and Instructional Guides. Teachers are encouraged to further incorporate the use of technological resources into their lesson plans.

The superintendent shall ensure that school system computers with Internet access comply with federal requirements regarding filtering software, Internet monitoring and Internet safety policies. The superintendent shall develop any regulations and submit any certifications necessary to meet such requirements.

A. REQUIREMENTS FOR USE OF TECHNOLOGICAL RESOURCES

The use of school system technological resources, such as computers and other electronic devices, networks, and the Internet, is a privilege, not a right. Before using the Internet, all students must be trained about appropriate on-line behavior. Such training must cover topics such as cyberbullying and interacting with others on social networking websites and in chat rooms.

Anyone who uses school system computers or electronic devices or who accesses the school network or the Internet at an educational site must comply with the requirements listed below. All students and employees must receive a copy of this policy annually. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges. Willful misuses may result in disciplinary action and/or criminal prosecution under applicable state and federal law

1. School system technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to activities that support learning and teaching. Use of school system technological resources for commercial gain or profit is prohibited.

2. Under no circumstance may software purchased by the school system be copied for personal use.

3. Students and employees must comply with all applicable board policies, administrative regulations, and school standards and rules in using technological resources. All applicable laws, including those relating to copyrights and trademarks, confidential information, and public records, apply to technological resource use. Any use that violates state or federal law is strictly prohibited.

4. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing or considered to be harmful to minors.

5. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).

6. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, students must not reveal personally identifiable, private or confidential information, such as the home address or telephone number, of themselves or fellow students.

7. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software or computer networks. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses.

8. Users may not create or introduce games, network communications programs or any foreign program or software onto any school system computer, electronic device or network without the express permission of the technology director or designee.

9. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.

10. Users are prohibited from using another individual's computer account. Users may not read, alter, change, execute or delete files belonging to another user without the owner's express prior permission.

11. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access

12. Teachers shall make reasonable efforts to supervise a student's use of the Internet during instructional time.

13. Views may be expressed as representing the view of the school system or part of the school system only with prior approval by the superintendent or designee.

B. RESTRICTED MATERIAL ON THE INTERNET

The board is aware that there is information on the Internet that is not related to the educational program. The board also is aware that the Internet may provide information and opportunities to communicate on subjects that are not suitable for school-age children and that many parents would find objectionable. School system personnel shall take reasonable precautions to prevent students from having access to inappropriate materials, such as violence, nudity, obscenity or graphic language that does not serve a legitimate pedagogical purpose. The superintendent shall ensure that the Internet service provider or technology personnel have installed a technology protection measure that blocks or filters Internet access to audio or visual depictions that are obscene, that are considered pornography or that are harmful to minors. School officials may disable such filters for an adult who uses a school-owned computer for bona fide research or another lawful educational purpose. School system personnel may not restrict Internet access to ideas, perspectives or viewpoints if the restriction is motivated solely by disapproval of the ideas involved.

C. PRIVACY

No right of privacy exists in the use of technological resources. School system administrators or individuals designated by the superintendent may review files, monitor all communication, and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School system personnel shall monitor on-line activities of individuals who access the Internet via a school-owned computer.

D. PERSONAL WEBSITES

The superintendent may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize school system or individual school names, logos or trademarks without permission.

1. Students

Though school personnel generally do not monitor students' Internet activity conducted on non-school system computers during non-school hours, when the student's on-line behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy (see the student behavior policies in the 4300 series).

2. Employees

All employees must use the school system network when communicating with students about any school-related matters. Thus, employees may not use personal

websites or on-line networking profiles to post information in an attempt to communicate with students about school-related matters.

Employees are to maintain an appropriate relationship with students at all times. Employees are encouraged to block students from viewing personal information on employee personal websites or on-line networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. If an employee creates and/or posts inappropriate content on a website or profile and it has a negative impact on the employee's ability to perform his or her job as it relates to working with students, the employee will be subject to discipline up to and including dismissal. This section applies to all employees, volunteers and student teachers working in the school system.

Legal References: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq.*; 20 U.S.C. 6777; G.S. 115C-325(e), -391

Cross References: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Copyright Compliance (policy 3230/7330), Web Page Development (3227/7322), Student Behavior Policies (all policies in the 4300 series), Public Records – Retention, Release and Disposition (policy 5070/7350), Use of Equipment, Materials and Supplies (policy 6520), Network Security (policy 6524), Staff Responsibilities (policy 7300)

Issued: December 11, 2002

Revised: January 9, 2008; October 14, 2009

Appendix F

REVISED MAY 24, 2010
Descriptor Term: Descriptor Code:
TECHNOLOGY ACCEPTABLE USE AND INTERNET SAFETY -- 7.1310
EMPLOYEES
Legal References:
Cross References:

In the 21st Century, technology tools and electronic resources are an integral part of a comprehensive educational program. Through these, both students and staff are able to extend classrooms beyond the four walls of their schools, enriching experiences and communicating on a global level. Computers, other electronic devices, programs, networks and the Internet support instruction, appeal to different learning styles and meet the educational goals of the board.

Use of technological resources should be integrated and infused into the system's educational program.
These resources should be used in teaching the North Carolina Standard Course of Study and in incorporating national curriculum standards. They also support valid business uses and provide for efficient work-related communication. This policy defines employees' proper conduct and responsibilities while using any school system electronic information resources. Employees are defined as all teachers, administration, and staff. This policy also applies to any other users who are expressly authorized by the board to use electronic information resources, including, but not limited to, board members, contractors, consultants, and temporary workers. Electronic information resources are defined as all computer equipment, peripherals, or other hardware that is owned or leased by the school system; user accounts (e.g. email, Novell, Active Directory); and any software licensed to the board.

Users must acknowledge that access and use of all board electronic resources is considered a privilege and not a right. Misuse of these resources may result in loss of this privilege as well as possible disciplinary or legal action.

It is the policy of the board to:

1. prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;

2. prevent unauthorized access and other unlawful online activity;

3. prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

4. comply with the Children's Internet Protection Act [Pub. L. No. 106-544 and 47 USC 254(h)].The superintendent shall ensure that school system computers with Internet access comply with federal requirements regarding filtering software, Internet monitoring and Internet safety policies. The superintendent shall develop any regulations and submit any certifications necessary to meet such requirements.

A. APPROPRIATE USE

All users are expect to exercise good judgment, use computer resources in a professional manner, and adhere to this policy and all applicable laws and regulations. Use of electronic information resources is expected to be related to the school system's goals of educating students and/or conducting school system business. The board recognizes, however, that some personal use is inevitable, and that incidental and occasional personal use that is infrequent or brief in duration is permitted so long as it occurs on personal time, does not interfere with the employee's work or school system business, and is not otherwise prohibited by board policy or regulations, procedures, or applicable law.

B. HARDWARE AND SOFTWARE

The board's comprehensive network is comprised of servers, computers, printers, peripherals, switches, routers, software and other devices. These resources are installed and maintained by members of the board's Information and Technology Department. Staff members shall not attempt to perform installation and maintenance without permission of the board's Technology Department. Users are prohibited from connecting any personal technologies to system owned and maintained local, wide, or metro area networks without permission of the board. These include computers, wireless access points and routers, printers, iPods, smart phones, PDAs. Software is licensed to the board by a large number of vendors and may have specific license restrictions regarding copying or using a particular program. Users must obtain permission from the Information and Technology Department prior to copying or loading school system software onto any computer, whether the computer is privately owned or is a board computer.

The use of software not owned or authorized by the board on any school system computers (including laptops, desktops, and the network) is discouraged. Prior to loading any software not owned or authorized by the board, an employee must receive express permission from the Information and Technology Department. The use of such software will be subject to any restrictions specified by the software license and to any restrictions imposed by the Technology Department. All software must be legally licensed by the user or the board prior to loading onto school system equipment. The unauthorized use of and/or copying of software is illegal.

The board's network may not be used for downloading entertainment software or other files not related to the mission and objectives of the board. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the instructional and administrative purposes of the board.

C. PROHIBITED USES
The following uses are prohibited uses of school system computers:

1. Commercial Use: Using school system computers for personal or private gain, personal business, or commercial advantage is prohibited.

2. Political Use: Using school system computers to advocate, directly or indirectly, for or against legislation, a ballot proposition and/or the election of any person to any office is prohibited.

3. Illegal or Inappropriate Use: Using school system computers for illegal, harassing, vandalizing, or inappropriate purposes, or in support of such activities, is prohibited. Illegal activities are any violations of federal, state, or local laws and include, but are not limited to, copyright infringement and/or illegal file sharing; committing fraud; threatening another person; or intentionally engaging in communications for the purpose of abusing, annoying, threatening, terrifying, harassing, or embarrassing another person.

Harassment includes, but is not limited to, slurs, comments, jokes, innuendoes, unwelcome compliments, cartoons, visual depictions, pranks, or verbal conduct relating to an individual that (a) have the purpose or effect of creating an intimidating, hostile or offensive environment; (b) have the purpose or effect of unreasonably interfering with an individual's work or school performance; or (c) interfere with school operations. Vandalism is any attempt to harm or destroy an operating system, hardware, application software, or data. Inappropriate use is any violation of other provisions of this policy and includes, but is not limited to, using another person's ID or password; plagiarizing; accessing, producing, storing, posting, sending, displaying, or viewing inappropriate or offensive material, including pornographic, obscene, discriminatory, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually suggestive language or images, or images of exposed private body parts; and accessing material advocating illegal acts or violence, including hate literature.

4. Unauthorized Use: School system computers may only be used by staff and students, and others expressly authorized by the Information and Technology Department.

5. Disruptive Use: Board computers may not be used to interfere with or disrupt other users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising ("spam"), propagation of computer viruses, distribution of large quantities of information that may overwhelm the system (chain letters, network games, or broadcasting messages), and any unauthorized access to or destruction of school system computers or other resources accessible through the network ("cracking" or "hacking"). Disruptive use may also be considered inappropriate and/or illegal. The following are considered disruptions and are also prohibited: posting personal or private information about the user or other people on the Internet; arranging or agreeing to meet with someone the user has met online for purposes other than official school business; attempting to gain unauthorized access to the board's network; posting information that

could be disrupting, cause damage, or endanger students or staff; and accessing chat-rooms or instant messaging software, unless for a valid educational purpose or official school business.

D. STAFF WEBSITES

The board provides numerous avenues through which teachers can facilitate their instructional programs. SharePoint, the board's web portal, provides each teacher with his/her own web site where instructional information should be posted. The board's XServe enables teachers to set up wikis and blogs to promote interaction with students. The board's Virtual Learning Environment (VLE) portal is the approved venue for hosting system-created online courses and supplemental content. All content posted on these sites remains the intellectual property of the board. There are numerous outside web sites where employees can bookmark and compile information to support their instructional goals. These sites are not appropriate venues to serve as substitutes for the employees' of the board's SharePoint, XServe, and VLE servers. Information posted on outside sites becomes the property of the site and the employee no longer has ownership or control of content. For this reason employees may not use these sites to post information for students.

The board recognizes that social networking sites can provide an important avenue of communication between staff, students, and parents. An employee who wants to utilize these sites must set up a board account that is separate from the employee's personal social networking site. Staff may use these system-specific sites to post announcements for parents, students and the community; they may not use these sites for posting instructional information. Employees are to maintain an appropriate relationship with students at all times. Employees are encouraged to block students from viewing personal information on employee personal websites or online networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. If an employee creates and/or posts inappropriate content on a website or profile and it has a negative impact on the employee's ability to perform his/her job as it relates to working with students, the employee will be subject to discipline up to and including dismissal. This section applies to all employees, volunteers and student teachers working in the school system.

E. COMPLIANCE WITH POLICY

This policy is applicable to all employees of the board and refers to all electronic information resources whether individually controlled, shared, stand-alone, or networked. Disciplinary action for employees shall be consistent with board policies and practices. Violation of this policy may constitute cause for revocation of access privileges, suspension of access to school system computers, dismissal and/or appropriate disciplinary or legal action.

F. STUDENT MONITORING RESPONSIBILITIES

School administrators and staff are responsible for reading the Student Acceptable Use Policy and for enforcing the policy for any and all students at the site in which they work. Administrators and staff must supervise student use of electronic information resources

and technology equipment in a manner that is appropriate to the students' age and circumstances of use.

G. MONITORING/NO EXPECTATION OF PRIVACY

The board's electronic information resources, the Internet, and use of email are not inherently secure or private. Employees shall have no expectation of privacy while using school system electronic information resources. The board reserves the right to search data or email stored on all school-owned or leased computers or other electronic information resources at any time for any reason. The board reserves the right to monitor employees' use of school system electronic information resources and to take appropriate disciplinary action based on the employees' inappropriate or illegal use or use that is in violation of this policy. The board reserves the right to disclose any electronic message to date to law enforcement officials, and under some circumstances, may be required to disclosed information to law enforcement officials or other third parties, for example, in response to a document production request made in a lawsuit involving the board or pursuant to a public records disclosure request.

H. SECURITY/CARE OF PROPERTY

Security on any computer system is a high priority, especially when the system involves many users. Employees are responsible for reporting information security violations to appropriate personnel. Employees should not demonstrate the suspected security violation to other users. Unauthorized attempts to log onto any school system computer on the board's network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a security risk or having a history of problems with other systems may be denied access.

Users of the board's technology equipment are expected to respect school system property and be responsible in using the equipment. Users are to follow all instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for computers while under their control. The school system is responsible for any routine maintenance or standard repairs to school system computers.

I. NO WARRANTIES

The board makes no warranties of any kind, whether express or implied, for the electronic information it is providing. The board will not be responsible for any damages suffered by users, including a loss of data resulting from delays, non-delivery, service interruptions, or any other cause. The board will not be responsible for any claims, losses, damages, costs, or other obligations arising from the unauthorized use of school system electronic information resources. Use of any information obtained via the Internet is at the user's risk. The board specifically denies any responsibility for the accuracy or quality of information obtained through its service. Users are responsible for any losses sustained by the board resulting from the user's intentional misuse of the school system's electronic information resources.

J. APPLICATION OF PUBLIC RECORDS LAW

All information created or received for work purposes and stored on or contained in the school system's computer resources or electronic data files is subject to public disclosure unless an exception to the Public Records Law applies. This information may be purged or destroyed only in accordance with the applicable records retention schedule and the State Division of Archives regulations. Staff email accounts will be archived for a minimum of three years.

K. EMPLOYEE AGREEMENT FORM

An Employee Acceptable Use Policy Agreement Form, developed by the school system, must be signed by the employee before access is permitted and an email account is assigned. An employee's acceptance of the Agreement is considered a condition of employment and refusal to sign may result in discipline up to and including dismissal.

Please fill in the form below and return the form to the school designee or to Human Resources.

School #5 Staff Acceptable Use and Internet Safety Policy
Board Policy 7.1310
Employee agreement:

I understand and will abide by the above School #5 Staff Acceptable Use and Internet Safety Policy. I further understand that any violation may result in the loss of access privileges and in disciplinary action.

Employee Name (please print) _____

Employee Signature _____

Date _____

School or Work Site _____

This agreement shall remain in effect as long as the staff member is employed by School #5 or until subsequent policy revision by the Board of Education.

Appendix G

School #6
Acceptable Use Policy
(PL 106-554)

The School #6 has the ability to enhance the education of students through the use of computers. The schools offer electronic network access for students, teachers, and staff within the school system.

SCHOOL #6 is pleased to offer students access to rich information resources through the electronic networks. We recognize that as telecommunications and other technologies shift the ways that information may be accessed, communicated, and transferred by members of society, those changes may also alter instruction and student learning. In a free and democratic society, access to information is a fundamental right of citizenship. Electronic information research skills are now fundamental to preparation of citizens and future employees.

One component of the access is the Internet, an electronic highway connecting thousands of computers, computer networks, and individual subscribers around the world. The Internet offers vast, diverse, and unique information resources previously unavailable to our schools. The network is provided for students and teachers to conduct research and communicate with others.

Goals for the utilization of the electronic network are to:

- Support the School #6 curriculum, the North Carolina Standard Course of Study, and the Vocational/ Technical Education Programs of Study
- Promote educational excellence in schools by facilitating resource sharing, innovation, and communication
- Enhance learning opportunities by focusing on information retrieval, searching strategies, research skills, and critical thinking
- Expand capabilities for learning opportunities
- Promote lifelong learning

Through the Internet, students, teachers, and staff will be able to have access to:

- Current information on topics such as countries of the world, elections, weather, etc.
- News from sources such CBS, ABC, CNN, and the New York Times
- Resources from businesses such as Dow Jones, Nations and First Union Banks, and Microsoft
- The Library of Congress and the State Library of North Carolina, as well as public, college, and university libraries
- Educational institutions such as the Public Schools of North Carolina, NCSU, UNC-Chapel Hill, ASU, Duke, and all other national and international universities with electronic access
- Government agencies, museums, and galleries including the Smithsonian, the Center for Disease Control, and NASA
- Research institutions and associations such as the World Health Organization, Alzheimer's Association, and National Council of Teachers of English

- A variety of other sources such as the Louvre, the Discovery Channel, Stanford's University Test Preparation site, ERIC, and the Whit House
- Public domain software and shareware of all types

Access to electronic mail and the Internet will enable students to explore thousands of libraries, databases, and bulletin boards while exchanging messages with Internet users throughout the world. Families should be warned that a small amount of material accessible via the Internet may contain items that are illegal, controversial, defamatory, inaccurate, or potentially offensive to some people. While our intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials that may not be considered to be of educational value in the context of the school setting. Users (and parents of users, if the user is under 18 years old) must understand that the School #6 cannot control the content of the information available on the Internet. We firmly believe that the valuable information and interaction available on this worldwide network far outweigh the possibility that users may encounter material that is not consistent with the educational goals of the system. We do not condone the use of such materials and take all reasonable precautions to limit access to these materials by using software programs that may block the material, by providing adult guidance and supervision, and by training students K-12 to use the network responsibly. Within reason, freedom of speech and access to information will be honored. The Internet is a tool that requires responsible users who control themselves. Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. The guidelines are provided here so that all are aware of the responsibility to which the users agree. Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply. School employees, students, and parents must be aware that access to the Internet will be withdrawn from users who do not respect the rights of others or who do not follow the rules and regulations established by the School #6 and their individual school.

Rules and Regulations

I. Acceptable Use: School #6 networks are to be used in a responsible, efficient, and legal manner and must be in support of the educational objectives and student behavior guidelines of the School #6. General school rules for behavior, communications and discipline apply as outlined in Board Policy JBC & JD and in Student Handbooks. Transmission of any material in violation of any federal or state regulation is prohibited.

Unacceptable uses include, but are not limited to, the following:

- Violating copyright laws
- Using network resources to commit plagiarism
- Reposing (forwarding) personal communications without the author's prior consent
- Using threatening or obscene material
- Distributing material protected by trade secrets Utilizing the network for commercial purposes
- Providing political or campaign information
- Mass email distribution (email may be sent to multiple known recipients if selected individually)
- Installation of software, unless approved by SCHOOL #6 Technology staff

- Using or attempting network resources to inappropriately distribute classroom material
- Using or attempting to use network resources to intrude, or hack, SCHOOL #6 or other networks

II. Netiquette: Users must abide by network rules. These rules include, but are not limited to, the following:

- Be polite - rudeness is never acceptable.
- Use appropriate language - do not swear or use vulgarities or any other abusive or inappropriate language.
- Illegal activities are strictly forbidden.
- Do not reveal your personal address or telephone number or those of anyone else.
- Never reveal credit or checking account information or social security numbers over the network.
- Do not disrupt the use of the network.
- Do not attempt to gain unauthorized access to system programs or computer equipment.
- Assume that all communications and information accessed via the network are private property and are subject to copyright laws.
- Notify the system administrator when a problem is identified.

III. Privileges: The use of the School #6 networks is a privilege, not a right. Access to network services, the Internet, and an email account will be given to students who agree to act in a considerate and responsible manner, and who abide by the Acceptable Use Policy. Inappropriate use will result in limitation or cancellation of user privileges and possible school disciplinary action. Each student who requests an individual account will be informed as to proper use of the network. Access to the Internet and an email account will be provided through individual schools.

IV. Disclaimer: The School #6 will not be responsible for any damages suffered, including the loss of data resulting from delays, non-deliveries, service interruptions, or inaccurate information. The user accepts personal responsibility for any information obtained or delivered via the network, including the prohibited sharing of personal information such as home address, checking account, and credit card information.

V. Security: Security on any computer system is a high priority, especially when the system involves many users. Attempts to log into the system as any other user or share a password will result in cancellation of user privileges. If a security problem is identified, notify the system administrator at the school. Do not demonstrate the problem to other users. Note that electronic mail is not guaranteed to be private; system operators have access to all mail. Messages relating to or in support of illegal activities will be reported to the authorities.

VI. Vandalism: Vandalism is defined as any malicious attempt to harm or destroy equipment, programs, and/or data of anyone connected to the server and or the Internet. This includes, but is not limited to, uploading, creating, or transmitting computer viruses. Vandalism will result in cancellation of user privileges and school disciplinary action.

VII. Accounts: Students may request individual, independent accounts. As these accounts become available, school rules will govern their use. Students should not assume that information in these accounts will always be private.

VIII. Privacy: Network administrators may review files and communications to maintain system integrity and insure that users are using the systems responsibly. Users should not assume that files stored on district servers and hard drives of computers will always be private.

IX. Web Site: On occasion, School #6 would also like to recognize and publish student artwork, writing, and/or photographs on our schools site on the World Wide Web. We further understand that the work will appear with a copyright notice prohibiting the copying of such work without express written permission. No name or personal information will appear with such photos and work unless the parent is notified. A parent may complete and sign a request for denial prohibiting the student to have access to the network, or recognition of work or photos published on the School #6 website.

These guidelines are provided so that the user and parents are aware of the responsibilities for the user. The School #6 supports and respects each family's right to decline the right to use network privileges.

If a School #6 user violates any of these provisions, his or her account will be terminated and future access could be denied. The signature(s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance.

STUDENT APPLICATION FOR INDEPENDENT USE OF NETWORKS
(Request for individual account)

Student name (please print):
_____

Date: _____ School:
_____

Current Grade: _____ Homeroom teacher:
_____

- ☐ new account
- ☐ renew account

Student Agreement

I have read and understand the District #6's Acceptable Use Policy for students. I agree to abide by the above Rules and Regulations for School #6 networks. I further understand that any violation is unethical and may constitute a school or criminal offense. Any violation will result in the loss of network access privileges, school disciplinary action and/or appropriate legal action. **I would like to apply for network privileges to access school files**

and to use for creation of personal electronic files in a secure storage location for my school work.

Student Signature _____

This space reserved for system administrator

Assigned user name _____

Assigned temporary password _____

Parent or Guardian Denial Form

Internet Access

I have read the above Rules and Regulations for the School #6 Networks and understand that this access is designed for educational purposes only. Although Internet filtering software is in place to restrict access to inappropriate materials, it is impossible to block all inappropriate materials. I understand that any violation is unethical and may constitute a school or criminal offense. Any violation will result in the loss of Internet access privileges, school disciplinary action and/or appropriate legal action. **Therefore, I prohibit the use of Internet privileges for my child, etc.**

Student Name (Please print): _____

Parent or Guardian Name (Please print): _____

Parent or Guardian Signature: _____

School: _____ Date: _____

Student Work

I accept responsibility for the use of network privileges for my child, but do not give permission to use my child's artwork, writing, or work on the School #6 Website.

Student Name (Please print): _____

Parent or Guardian Name (Please print): _____

Parent or Guardian Signature: _____

School: _____ Date: _____

Student Photo

I accept responsibility for the use of network privileges for my child, but do not give permission to use my child's photo on the School #6 Website.

Student Name (Please print): _____

Parent or Guardian Name (Please print): _____

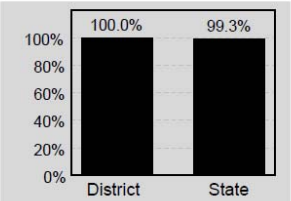
Parent or Guardian Signature: _____

School: _____ Date: _____

Appendix H (NC Report Card)

ACCESS TO TECHNOLOGY

Percentage of Classrooms Connected to the Internet



Number of Students per Instructional Computer

	NUMBER OF STUDENTS
District	1.65
State	2.72

Number of Students per Internet-Connected Computer

	NUMBER OF STUDENTS
District	1.65
State	2.74

Appendix I (NC E-Rate Example Audit - Draft)

Attachment A
Documents To Be Made Available

1. Technology plan(s), technology plan amendments, and technology plan approval letters covering the Funding Year(s) identified in the letter.

2. Approved budget(s) (or budget drafts) for the technology plans in item 1 above as well as for the applicant's non-discount share.

3. Note: Contracted auditors would ask for copies of audited financial statements for the Funding Year(s) identified in the accompanying letter and a copy of the most recent statements. It is not necessary to provide audited financial statements for the purposes of this "example-audit".

4. General description of the information technology environment and a high-level network diagram. (The description should include how S&L Program funding for internal connections is being used in the IT environment.)

5. Method used and documentation supporting the discount calculation.

6. Copies of your Internet Safety Policy and other documentation supporting compliance with the Children's Internet Protection Act (CIPA). (Including public notice/public hearing documentation.)

7. Fixed asset register or other records listing for all S&L Program funded equipment that was acquired and reimbursed during the Funding Year(s) identified in the letter.

    a. Make

    b. Model

    c. Serial Number

    d. Physical Location (including room number and movement history)

    e. Date Installed

    f. FRN

    g. Customer Invoice Reference Number(s)

8. Copies of all relevant contracts and written agreements with service providers and consultants for the period(s) indentified in the letter. (Including any amendments.)

9. Record Retention Policy that applied to and was followed for S&L Program documentation.

10. Copies of the following forms (if applicable) for the Funding Year(s) identified in the letter:

    a. FCC Form 470

    b. FCC Form 471

    c. FCC Form 486

    d. FCC Form 472 (if applicable)

    e. FCC Form 500 (if applicable)

11. All documentation associated with above FCC Form(s) 471 and selected FRN(s) to include, but not limited to, service substitution approval letters and equipment transfer notification letters to USAC.

12. When FCC Form 472 (BEAR) is used:

    a. Copy of canceled checks written to the service provider

    b. Copy of bank statement and any other supporting documentation to confirm receipt of the discounted portion from the service provider

13. When FCC Form 474 (SPI) is used, copy of canceled check written to the service provider to cover the non-discounted portion.

14. Copies of local and state procurement regulations pertaining to contracting for the purchase of telecommunications, Internet access, internal connections, and basic maintenance of internal connections.

15. Copies of all information related to the service provider selection process including, but not limited to:

    a. RFPs or bidding specifications

    b. All bids received (both winning and losing)

    c. All correspondence (including informal communications) with potential selected service providers

    d. Bid evaluation worksheets

    e. Memorializations (i.e. no responses, existing contract, etc.)

f. Meeting minutes for discussions and selection of service providers

16. Copy of relevant meeting minutes during the period(s) being examined were the S&L Program was an agenda item.

17. Copies of contract(s) and/or invoices for the technology protection measure (i.e. Internet filter) in place during the Funding Year(s) identified in the letter.

18. Copies of filtering logs for the technology protection measure in place during the Funding Year(s) identified in the letter.

19. Relevant bills and invoices.

20. Note: Contracted auditors would ask for contact information for School Board Members, Superintendents, Principals (if beneficiary is an individual school), Finance Officer, and Consultant (if applicable).

21. Completed Internal Control Questionnaire (see Attachment B).

Vita

Alan Michael Warren was born in Gastonia, NC, on May 31st, 1983. He attended elementary school in Gastonia and Statesville, NC., and graduated from North Iredell High School in North Carolina in May of 2001. In the fall, he attended Western Carolina University to study Accounting, and in December of 2005 he was awarded a Bachelor of Business Administration degree. In the fall of 2006 he became a business education teacher with North Iredell High School and transferred to West Iredell Middle School in 2007. He became an Instructional Technology Specialist with Iredell-Statesville Schools in 2008 and attended Appalachian State University where he continues work towards a Masters of Instructional Technology.

Mr. Warren is a member of Kappa Sigma Fraternity. His home address is 196 Delight Loop. Statesville, NC. He is married to Jamie Bumgarner Warren of Cleveland, NC and his parents are Michael Wayne Warren of Statesville and Mrs. Susan Nivens Warren of Gastonia.